# Reprocessing of biometric data for law enforcement purposes

Jasserand-Breeman, Catherine

university of groningen

# Reprocessing of Biometric Data for Law Enforcement Purposes

Individuals' Safeguards Caught at the Interface between the GDPR and the 'Police' Directive?

**PhD thesis**

to obtain the degree of PhD at the
University of Groningen
on the authority of the
Rector Magnificus prof. E. Sterken
and in accordance with
the decision by the College of Deans.

This thesis will be defended in public on

Thursday 11 July 2019 at 11.00 hours

by

**Catherine Agnès Jasserand-Breeman**

born on 3 March 1976
in Tassin La Demi-Lune, France

## Supervisors

Prof. G.P. Mifsud Bonnici
Prof. L.W. Gormley

## Assessment Committee

Prof. J.A. Cannataci
Prof. Y. Poullet
Prof. F. Boehm

**Acknowledgements**

This PhD dissertation would not have been possible without the help and support of many people who surrounded me during this long journey. My first thanks go to my supervisors, Professor Jeanne Mifsud Bonnici and Professor Laurence Gormley. Jeanne, I would like to thank you for the flexibility that you offered me to explore many research paths and for your enthusiasm when I presented unconventional ideas. You had the patience to listen to me while guiding me on the right track when I felt lost in my research. Laurence, I am grateful for your commitment to enabling me to reach my goals and for your attention to detail. I still remember the warm welcome that you gave me the day of my job interview at the University.

I also thank the Faculty of Law for the arrangement they agreed on during the PhD. A special thanks to the Graduate School and, in particular, to Marjolijn Both, Anita Kram, and Professor Pauline Westerman for the fantastic job that you do in supporting PhD students. I am grateful to my assessment committee, composed of Professor Franziska Boehm, Professor Yves Poullet, and Professor Joe Cannataci, for reading my thesis and allowing me to defend it.

Besides, the research would not have been possible without the funding provided by INGRESS, an EU-FP7 project on the development of fingerprint sensors. For more than three years, the project offered me the opportunity to discuss various technical issues linked to the development of biometric technologies. Special thanks to Aurélie Moriceau, Stéphane Revelin, Marina Pouet, Egidijus Auksorius, Martin Olsen, Kiran Raja, Professor Christophe Champod, Professor Christoph Busch, Alexandre Anthonioz, Berkay Topcu, Nenad Marjanovic, Marc Schnieper, Serena Papi, Agnieszka and Wielsaw Bicz. I hope to have the opportunity to pursue cross-disciplinary research with you in the future.

A special thanks to Els Kindt. Els, you introduced me to your network of professionals in the biometric field and recommended me as a speaker for several conferences organised by the European Biometrics Association. Thank you for your trust and for sharing your expertise.

I am grateful to several researchers who gave me a bit of their precious time to discuss various issues and, in particular, to Peel Geelhoel whose knowledge on criminal law helped me to think outside the 'data protection' bubble, Professor Arun Ross for lengthy discussions on how and whether we could bridge the gaps between the scientific and technical communities, and Professor Sébastien Marcel for exchange on facial recognition technologies.

I also thank my past and present colleagues at STeP, who took the time to chat, exchange ideas, share their office, or go out for dinners each time I was in Groningen. Thank you Aukje, Melania, Oskar, Frank, Bo, Evgeni, Jonida, Carolin, Gerard (also for kindly translating the summaries in Dutch!), Nynke, Trix, Karen, Lauren, Nati, Styliana, Warsha, Bettina, and Joe. Colleagues from the European Law Department also belong to this list: Karien (a special thanks for your help, kindness, and patience), Matthijs, Martin, Laurenzo, Hans, and Peter. Dimitry, with your sense of humour, the intellectual discussions that you liked to provoke, and your colourful ties, you naturally have a place in this list.

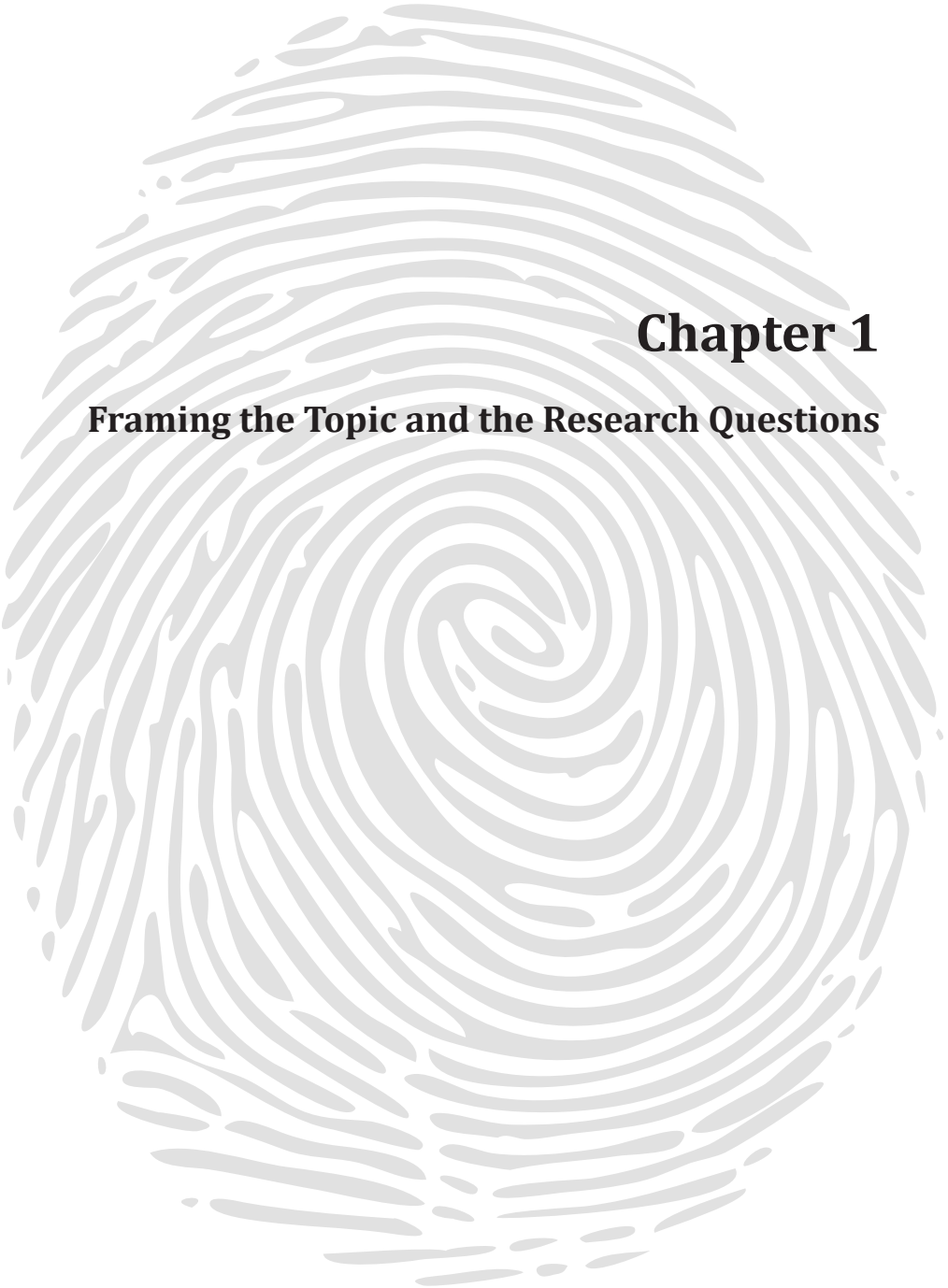
I also have in mind my ex-colleagues from IViR, where I started research several years ago. Esther and Bart, I miss our lunch dates. Ana, Christina, and João Pedro, thank you for your advice, suggestions, and kind words.

Finally, I want to thank my family-in-law, Ans, Dolf, and Ilse for their precious help each time I needed to travel to Groningen or other places for conferences.

This dissertation is also dedicated to my *parents chéris*, Françoise and Jean-Paul, who have always pushed us to be intellectually curious. To my brothers, Patrick and Jean-Philippe (with Carine, Hippolyte, Maxence, and Callixte), and my sister, Laëticia, thank you for helping me keep my feet on the ground.

To Raphaël and Tim, my sweet boys who had enough patience with me throughout the years and who reminded me that *there is more to life than books*. Last but not least, to my husband, Dirk-Jan, for his logistic and mental support, as well as for the faith that he had in me from the start of the project. Thank you, this dissertation would have never seen the light of day without you!

## *Table of Contents*



# Chapter 1

## Framing the Topic and the Research Questions

## *Chapter 1: Framing the Topic and the Research Questions*

### I. Introduction

Biometric technologies are very present in our daily lives. Limited for a long time to the fields of law enforcement and border controls, biometric technologies are now commonly used by the private sector. Fingerprints, face, voice or iris data are used, among others, to book payments, give access to work premises or unlock mobile devices.[1] By 2020, banks are estimated to offer biometric services to more than 1,9 million customers.[2]

Besides the growing use of biometric data by private parties, another trend has emerged thanks to the 'vast trove of personal data' that social media and online platform hold.[3] Among the data collected are facial images (photographs, videos) and voice samples (videos or audio messages), which can be reprocessed for biometric recognition purposes. Mark Zuckerberg, the Facebook's CEO, has recently acknowledged that the social network processes the photographs uploaded onto the platform for facial recognition purposes.[4] A few years ago, the company developed facial recognition software to match people's pictures with friends' names and encouraged users to identify people that looked like their friends.[5] After complaints from the Irish and the Hamburg Data Protection Authorities,[6] Facebook deactivated the 'tag' feature in Europe,[7] but the company announced in April

[1] Ethan Ayer, 'How Government Biometrics are Moving into the Private Sector' (*Biometric Update*, 28 June 2017)<https://www.biometricupdate.com/201706/how-government-biometrics-are-moving-into-the-private-sector> accessed 30 September 2018.

[2] Xavier Larduinat, 'Biometrics and the Next Financial Sector Revolution' (*blog.Gemalto*, 22 May 2018) <https://blog.gemalto.com/financial-services/2018/05/22/biometrics-and-the-next-financial-sector revolution/> accessed 30 September 2018; Business Wire, 'The Biometrics for Banking: Market and Technology Analysis, Adoption Strategies and Forecasts 2018-2023- Second Edition' (*businesswire.com*, 29 June 2018) <https://www.businesswire.com/news/home/20180629005676/en/Biometrics-Banking-2018-Market-Technology-Analysis-Adoption> accessed 30 September 2018.

[3] The expression of 'vast trove' is commonly used in relation to the exploitation of collected data by social media, see for instance Somini Sengupta, 'Facebook's Prospects May Rest on Trove of Data' *New York Times* (14 May 2012) <https://www.nytimes.com/2012/05/15/technology/facebook-needs-to-turn-data-trove-into-investor-gold.html?pagewanted=all> accessed 30 September 2018.

[4] Steve Andriole, 'Facebook's Zuckerberg Quietly Drops Another Privacy Bomb-Facial Recognition' *Forbes* (12 April 2018) <https://www.forbes.com/sites/steveandriole/2018/04/12/facebooks-zukerberg-quietly-drops-another-privacy-bomb-facial-recognition/#27ebe7fe51c0> accessed 30 September 2018.

[5] For example, Ingrid Lunden, 'Facebook Turns Off Facial Recognition in the EU, Gets the All-Clear On Several Points from Ireland's Data Protection Commissioner on its Review' *TechCrunch* (21 September 2012) <https://techcrunch.com/2012/09/21/facebook-turns-off-facial-recognition-in-the-eu-gets-the-all-clear-from-irelands-data-protection-commissioner-on-its-review/> accessed 30 September 2018.

[6] For instance, Press Association, 'Facebook Faces Fines up to £80K' *The Guardian* (21 September 2012) <https://www.theguardian.com/technology/2012/sep/21/facebook-faces-privacy-fine> accessed 30 September 2018; Helen Pidd, 'Facebook Facial Recognition Software Violates Privacy Laws, says Germany' *The Guardian* (3 August 2011) <https://www.theguardian.com/technology/2011/aug/03/facebook-facial-recognition-privacy-germany> accessed 30 September 2018.

[7] Tim Bradshaw, 'Facebook Ends Facial Recognition in Europe' *Financial Times* (21 September 2012) <https://www.ft.com/content/fa9c4af8-03fc-11e2-b91b-00144feabdc0> accessed 30 September 2018.

2018 its intent to reintroduce it in Europe based on users' consent.[8] In addition, to test its facial matching algorithms, the social media has set up a private facial recognition database for research purposes. But Facebook is not the only one to process for biometric purposes the data of its users. Google has also developed its own large-scale facial database fed by the photographs it holds.[9] Besides, the Internet search engine enables its users to record their voice and audio activities. One of the purposes of the 'Google Voice and Audio' function is precisely to allow the company to use individuals' voices to improve its speech recognition systems.[10]

Facial images and voice samples held by social networks are particularly valuable to law enforcement authorities as they allow the identification of individuals based on the distinctive characteristics of their body (e.g. face geometry) or behaviour (e.g. voice tone, accent). As reported by the transparency reports of the big tech companies (including Facebook and Google), the requests made by law enforcement authorities to access users' accounts and content have increased through the years.[11] Although the reports do not disclose the types of content requested and obtained, one could assume that law enforcement authorities request access to pictures, videos and voice samples, to further process them including for biometric recognition purposes.[12]

Law enforcement authorities can have access to biometric data through different channels. They can directly collect them, for instance during a criminal investigation. They can request access to biometric data held in databases set up by public authorities for non-law enforcement purposes (such as databases constituted for border controls purposes). Or they can request access to biometric data held by private parties. It is on the latter case that the research focuses. The increasing volume of biometric data held by private parties and the adoption of new EU data protection rules justify such a choice. The research also builds on a trend that has grown over the years, raising concerns on its impacts on data

[8] Tyron Stewart, 'Facebook is Using GDPR as a Means to Bring Facial Recognition Back to Europe' *MobileMarketing* (18 April 2018) <https://mobilemarketingmagazine.com/facebook-facial-recognition-eu-europe-gdpr-canada> accessed 30 September 2018.

[9] According to Ira Kemelmacher-Schlizerman et al, several social media and online platforms have constituted private research facial database based on the photographs that they hold. FaceNet, the private database set up by Google for research purposes exclusively is deemed to be the biggest one containing more than 500 million pictures from more than 10 million individuals, as described in Ira Kemelmacher-Shlizerman et al, 'The MegaFace Benchmark: 1 Million Faces for Recognition at Scale' (2015) <https://arxiv.org/abs/1512.00596> accessed 30 September 2018.

[10] See Support Google on Google Voice and Audio Activity <https://support.google.com/websearch/answer/6030020?co=GENIE.Platform%3DDesktop&hl=en> accessed 30 September 2018.

[11] See for instance, Facebook's Transparency Report released in May 2018 <https://transparency.facebook.com/government-data-requests> accessed 30 September 2018; Google's Transparency Report <https://transparencyreport.google.com/user-data/overview > accessed 30 September 2018; Apple's Transparency Report, January – June 2017 <https://images.apple.com/legal/privacy/transparency/requests-2017-H1-en.pdf> accessed 30 September 2018; see also Microsoft's Transparency Report <https://www.microsoft.com/en-us/about/corporate-responsibility/lerr/> accessed 30 September 2018.

[12] See for instance, in the USA, Matt Cagle, 'Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color' *ACLU Northern California* (11 October 2016).

subjects' rights: the access to and re-use by law enforcement authorities of biometric databases initially constituted for a non-law enforcement purpose.

This tendency has been criticised by the European Data Protection Supervisor (EDPS), but mainly in relation to databases constituted for the asylum and border controls policies of the EU. As early as 2005, the EDPS warned against the risks posed by law enforcement 'systematic' access to databases constituted for a different purpose without specific justifications or safeguards.[13] It repeated its concerns in 2009 and 2012 when it reviewed the proposals to extend the scope of the asylum seekers' EU fingerprint database (the EURODAC) to law enforcement authorities.[14] In particular, it was concerned that the data at stake belonged to individuals not suspected of (having committed) any crime.[15] It also highlighted the challenges that such an extension of purpose posed to the principle of purpose limitation and warned against the risk of 'function creep.'[16] From that time onwards, the EDPS has not stopped reiterating its criticisms towards a trend that has been 'normalised.' For instance, in recent proposals on border controls, the European Commission has proposed 'from the start of the system' to provide law enforcement authorities access to foreign travellers' databases.[17] The Article 29 Data Protection Working Party (A29WP)[18] has also criticised and analysed this trend, including in its Opinion on the principle of purpose limitation.[19] The role of this principle, which constitutes one of the core elements of the research, is explained in greater details in the next chapters.

The research, however, does not focus on these public databases but on the trend of secondary use of biometric data originating from the private sector. More specifically it investigates the re-use of private-sector data by law enforcement authorities because it is assumed that data subjects might benefit from a different level of protection when their

[13] EDPS, 'Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM (2005) 600 final)' [2006] OJ C97/6, 6-7.
[14] EDPS, 'Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (.../...) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes' [2010] OJ C92/1.
[15] ibid 8.
[16] EDPS, 'Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] [...] (Recast version)' [2012], 7.
<https://edps.europa.eu/sites/edp/files/publication/12-09-05_eurodac_en.pdf>accessed 30 September 2018.
[17] EDPS, 'Opinion 06/2016, EDPS Opinion on the Second EU Smart Borders Package, Recommendations on the revised Proposal to establish an Entry/Exit System' [2016], 19-21.
[18] An independent body advising the European Commission on data protection matters, which is replaced by the European Data Protection Board with the entry into force of the new EU data protection rules.
[19] eg A29WP, 'Opinion 05/2013 on Smart Borders' [2013] WP206; as well as A29WP, 'Opinion 03/2013 on purpose limitation' [2013] WP203.

data are initially collected for a non-law enforcement purpose (such as an operational or commercial purpose) and further processed for a law enforcement purpose (such as in the context of a criminal investigation). The thesis focuses on biometric data because of their ability to distinctively identify individuals through their 'unique link' to an individual's body or behaviour.[20] Biometric data, which are the representations of biometric characteristics, have also been used for a long time by police authorities to identify individuals.[21] The novelty lies in the source of the data, which do not originate from law enforcement authorities but from the private sector.

Before the adoption of a comprehensive EU data protection framework, the rules applicable to the processing of personal data were split between the Data Protection Directive (Directive 95/46/EC) and a patchwork of instruments applicable to the processing of personal data in the area of police and judicial cooperation. This fragmented legal framework has been replaced by a general instrument applicable to the processing of personal data across sectors (the General Data Protection Regulation or GDPR)[22] and a more specific directive governing the processing of personal data in criminal and judicial contexts (Directive 2016/680 or the 'police' Directive).[23] The interface between the two instruments and its consequences on the safeguards granted to individuals are at the heart of the research.

## II. Research Questions

With the entry into force of the Lisbon Treaty,[24] the Charter of Fundamental Rights (the Charter) became a binding instrument having the same legal value as the Treaties.[25] The Charter proclaims fundamental rights, among which the right to the protection of personal data (Article 8 of the Charter). As detailed in the next section (theoretical framework), Article 8 of the Charter sets out the fundamental right to data protection and specifies the conditions under which personal data should be processed. Paragraph 2 of Article 8 provides, in particular, that:

[20] The alleged 'uniqueness' of biometric characteristics, challenged by forensics experts, is discussed in *Chapters 2* and *3* of the thesis.
[21] See for instance, the system of measurements of hands, feet, and other body's parts by Alfred Bertillon in the 19th Century, in Simon Cole, 'Measuring the Criminal Body', *Suspect Identities: A History of Fingerprinting and Criminal Identification* (Harvard University Press 2001) 32-59.
[22] European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and of the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
[23] European Parliament and Council Directive (EU) 2016/680 of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.
[24] Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C306/01.
[25] art 6 of the Treaty on European Union (TEU), see Consolidated Version of the Treaty on European Union [2016] OJ C202/13, 19.

> 'Such data [i.e. personal data] must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.'[26]

The fundamental right to data protection is fleshed out in secondary law, and in particular in the GDPR and the 'police' Directive. Due to the nature of the right and the type of personal data at stake, it is legitimate to investigate the guarantees or safeguards afforded to individuals whose personal data, held by private parties, are reprocessed by law enforcement authorities. The research question of the study is thus worded as follows:

> ***Which safeguards does the new EU data protection framework grant to individuals whose biometric data were initially collected by private parties and are subsequently processed for a law enforcement purpose by competent authorities?***

This main question is addressed through:

1) An investigation of the terminology and the legal nature of biometric data from an EU data protection perspective based on the following questions:

> *How is the notion of 'biometric data' defined and approached from a technological and a data protection perspective? How does the new data protection framework define the category of 'biometric data'? How different are biometric data from other types of personal data? Is there any specific protection attached to this category of personal data?*

2) A discussion on the interface between the GDPR and the 'police' Directive, as well as the indispensable assessment of the subsequent use of private-sector biometric data for law enforcement purposes, approached through the following questions:

> *Does the new data protection framework address the collection of personal data under one instrument (the GDPR) and their further processing under the other (the new Directive)? In this scenario, does the principle of purpose limitation play in any role in limiting or framing the access to and re-use of personal data initially collected for a different purpose?*
>
> *Are there any specific safeguards to protect individuals' rights? Do individuals have, for instance, the right to be informed of the subsequent use of their personal data? And how should these safeguards be mitigated with the interests pursued by law enforcement authorities?*

[26] Charter of Fundamental Rights of the European Union [2000] OJ C364/3, 10, see now [2016] OJ C202/389, 395.

3) An attempt to mitigate the risks to the individuals' right to data protection and define possible solutions based on the following questions:

> *Which role can the new tools of Data Protection by Design and Data Protection Impact Assessment play? Based on the findings of the previous questions and on the accountability tools provided by the new data protection framework, which recommendations can be made?*

## III. Methodology

This research is a legal study with an interdisciplinary component. The research question cannot be answered without understanding the field of biometric recognition. To that end, the researcher has collaborated with scientists (engineers and computer scientists) during the preparation of the research. The non-legal elements of the study provide necessary insights and are used as descriptive and explanatory elements.[27]

### 1. Interdisciplinary Component

The first set of questions investigates the context of the research, comparing the concept of 'biometric data' as defined in the new EU data protection framework with the technological notion, and assessing the impact of the new legal rules on biometric data processing. The first issue is addressed in two chapters, one on the terminology (*Chapter 2*) and the other on the legal nature of biometric data (*Chapter 3*).

To understand the field that the law regulates and the processing of biometric data, the research has relied on experts in the field. The purpose was to gain a basic knowledge of technical issues through informal discussions with scientists and the reading of scientific literature. Guided by experts, the researcher could identify 'topical' technological issues that could have an impact on data protection. For instance, for many years, it was believed that biometric templates (such as fingerprint templates) were anonymous data as they were a mathematical representation of fingerprint images and could not be traced back to the individual to whom the fingerprints belonged.[28] However, several researchers have shown that it is possible to reconstruct, though partially, a fingerprint image from a fingerprint template.[29] Taking into account the current state-of-the-art, it would be incorrect to state that fingerprint templates are anonymous data, and thus not personal data.

[27] The research follows in part the methodology described by Schrama in Wendy Schrama, 'How to Carry out Interdisciplinary Legal Research: Some Experiences with an Interdisciplinary Research Method' (2011) 7(1) Utrecht Law Review 147.
[28] See in particular, Jan Grijpink, 'Privacy Law: Biometrics and Privacy' (2001) 17(3) Computer Law & Security Review 154, 156.
[29] eg Kai Cao and Anil Jain, 'Learning Fingerprint Reconstruction: from Minutiae to Image' (2015) 10(1) IEEE Transactions on Information Forensics and Security 104.

To build the 'basic' scientific knowledge, the researcher has consulted handbooks, manuals, and encyclopedia in the field. In particular, the book 'Introduction to Biometrics' has constituted a sound reference during the research as it introduces critical topics such as terminology, security, privacy, biometric recognition techniques and modalities.[30] Completed with 'the 'Handbook on Biometrics' on different biometric technologies,[31] it provides a solid overview of the field and applicable modalities (face recognition, iris recognition, hand geometry recognition, or fingerprint recognition to name a few). Specialised handbooks on face recognition[32] and fingerprint recognition[33] have also been consulted for a deeper understanding of the topic. For a comprehensive overview, several entries in the 'Encyclopedia of Biometrics' have constituted useful references,[34] in particular, on the distinction between the verification and the identification process;[35] the harmonisation of the biometric vocabulary,[36] or the origins of the use of fingerprints in a criminal context.[37] The Encyclopedia contains more than one thousand entries that are either definitions or short descriptions of the concepts, systems, algorithms, techniques or modalities. Last, the research has also taken into account books presenting issues relating to biometric technologies from legal, ethical, and technological perspectives, such as 'Security and Privacy in Biometrics'[38] and 'Ethics and Policy of Biometrics.'[39]

Issues identified as essential for the research have been discussed with engineers and computer scientists who were partners in the EU-FP7 INGRESS project in which the researcher participated.[40] This project was dedicated to the development of new types of fingerprint sensors and involved collaboration between technical and legal experts. Some of these partners indicated relevant scientific literature in the field of fingerprint reconstruction.[41] The discussions have been very useful to determine, for instance, if a biometric template contains identifying information and could thus qualify as personal and/or biometric data. They have also helped establish the distinction between the concept of identification from a biometric recognition perspective and that from a data protection perspective. Those nuances are discussed in the next chapters of the thesis.

[30] Anil K Jain, Arun A. Ross, and Karthik Nandakumar (eds), *Introduction to Biometrics* (Springer 2011).
[31] Anil Jain, Patrick Flynn, and Arun Ross (eds), *Handbook of Biometrics* (Springer 2008).
[32] Stan Z Li and Anil K Jain (eds), *Handbook of Face Recognition* (2nd edn, Springer 2011).
[33] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar (eds), *Handbook of Fingerprint Recognition* (2nd edn, Springer 2009).
[34] Stan Z Li and Anil K Jain (eds), *Encyclopedia of Biometrics* (Springer 2015).
[35] eg James L Wayman, 'Biometric Verification/Identification/Authentication/Recognition: The Terminology' in *Encyclopedia of Biometrics* (n 34) 153-157.
[36] eg Rene McIver, 'Biometric Vocabulary Standardization' in *Encyclopedia of Biometrics* (n 34) 157-160.
[37] eg Davide Maltoni, 'Fingerprint Recognition, Overview' in *Encyclopedia of Biometrics* (n 34) 510-513.
[38] Patrick Campisi (ed), *Security and Privacy in Biometrics* (Springer 2013).
[39] Ajay Kumar and David Zhang (eds), *Ethics and Policy of Biometrics,* Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, IECB (Springer 2010).
[40] The INGRESS project (Innovative Technology for Fingerprint Live Scanners) ran from November 2013 to May 2017 under the grant agreement no 312792.
<http://www.ingress-project.eu> accessed 30 September 2018.
[41] See Cao and Jain (n 29).

**2. Legal Analysis**

The second set of questions addresses the normative issues raised by the research. It relies on a doctrinal analysis of the law, case law, guidelines and opinions in the field of EU data protection. As defined by Mann, doctrine 'explains, makes coherent or justifies a segment of the law as part of a larger system of law.'[42] According to Hutchinson and Duncan, 'doctrinal research is research into the law and legal concepts. This method of research was the dominant influence in 19th and 20th century views of law and legal scholarship, and it tends to dominate legal research design.'[43]

The research follows the Hutchinson and Duncan's two-step approach methodology, which consists in first finding the sources, and then interpreting and analysing them. The first step states what the law says, i.e. the GDPR and Directive 2016/680, whereas the second one interprets the provisions. The interpretation is made through the European Court of Justice (ECJ) case law on concepts originating from the previous data protection instrument, Directive 95/46/EC, and the European Court of Human Rights (ECtHR) jurisprudence on the scope of and limitations to the right to privacy as encompassing the right to data protection. The method is further described in the next section on the 'theoretical framework.'

Answers to the last set of questions are based on the accountability tools introduced in both instruments, namely the Data Protection by design and by default measures and the Data Protection Impact Assessment provision. This part relies on the interpretation given to the provisions by the European Data Protection Supervisor (EDPS) and the Article 29 Data Protection Working Party (A29WP).

The legal method used, together with specific references to the provisions, case law and opinions, is further detailed in the next section.

Finally, concerning the format of the thesis, the researcher has opted for a thesis by publications. First, the topic of the dissertation and the adoption of the new legal data protection framework during the research have justified the publication of the findings at an early stage of the research. Second, the submission and revision of the articles have helped the researcher refine her analysis and argumentation in a very technical field. Third, the objective of the researcher was to develop the necessary writing skills to pursue an academic career, while testing her findings on the new EU data protection framework.

[42] Trischa Mann (ed), *Australian Law Dictionary* (1st edn, OUP 2010) 197; Hutchinson and Duncan in Terry Hutchinson and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17(1) Deakin Law Review 83, 84.
[43] Hutchinson and Duncan, ibid 85.

## IV. Theoretical Framework

The study covers different areas: the data protection rules applicable to data processing for both law enforcement and non-law enforcement purposes, as well as the definition and processing of biometric data from data protection and technological perspectives. The key concepts and theories on which the research is based, a well as the legal framework, are described below.

### 1. Concepts and Theories

The research assesses the new EU data protection framework, which provides a statutory definition of the concept of 'biometric data' and applies specific rules to the processing of personal data for law enforcement purposes. This framework is adopted on the basis of the right to data protection enshrined in Article 8 of the Charter of Fundamental Rights.

#### *a. The EU Right to Data Protection as a Fundamental Right*

Even before the entry into force of the Charter of Fundamental Rights, the right to data protection was recognised by the ECJ as a fundamental right.[44] With the entry into force of the Charter, the right to data protection became a full-fledged, albeit not absolute, fundamental right.[45] Restrictions to EU fundamental rights are, indeed, permitted under specific conditions.[46] The main theory of the research is based on the scope of the fundamental right to the protection of personal data, also called the right to data protection.

Specific guarantees derive from the fundamental nature of the right to data protection, such as the data protection principles of fair processing and purpose specification, the requirement of a legal basis (either individuals' consent or other 'legitimate basis laid down by law'), and the data subjects' rights of access and rectification.[47] As set out in the general Article 52(1) of the Charter, fundamental rights can be limited under specific conditions. The limitations must be defined by law, respect the 'essence' of the right at stake, and comply with the principles of proportionality and necessity.[48]

Those conditions are based on the European Court of Justice's case law, as acknowledged in the non-binding explanations to the Charter.[49] After the entry into force of the Lisbon Treaty, and thus the binding application of the Charter, the ECJ acknowledged the 'relative'

[44] As acknowledged by the ECJ in its case law *Promusicae*, see Case C-275/06, *Productores de Música de España (Promusicae)* v *Telefónica de España SAU* [2008] ECLI:EU:C:2008:54, paras 63-65.
[45] Established by the ECJ's case law and art 52(1) Charter, as well as reflected in Recital 4 GDPR.
[46] art 52(1) Charter.
[47] art 8(2) Charter.
[48] art 52 of the Charter reads as follows:
'1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet the objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.'
[49] Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/17, 17-35.

nature of the right to data protection in the *Volker* case,[50] which it reiterated in *Schwarz* on the collection and storage of fingerprints in EU citizens' passports.[51] The Court stated that 'the right to the protection of personal data is not, however, an absolute right, but must be considered in relation to its function in society.'[52] The Court did not explain what this function is, but checked, instead, if the right to data protection had been infringed.[53] Commenting on this decision, Mifsud Bonnici has suggested three possible functions to the right to data protection: the first one is based on the control or autonomy that individuals might exercise on their personal data; the second on the 'trust' that data protection can inject in society, and the last one is linked to the role played by the right to enable citizens to participate in society.[54] To date, the ECJ has not discussed the matter. Instead, it seems that the Court has moved to the issue of the 'essence' of the right to data protection and the permitted limitations to the fundamental rights.[55] But since Recital 4 of the GDPR expressly refers to the ECJ's ruling,[56] the ECJ might have to specify, at a point in time, what the function of the right to data protection in society is.

The current research thus acknowledges the non-absolute nature of the right to data protection and its possible limitations for law enforcement purposes, through the analysis of case law. However, the focus of the study is not on the justifications of these limitations but on the safeguards given to individuals when their personal data – being biometric data in the situation at stake - are re-used by law enforcement authorities. The research investigates the issues from the perspective of the data subjects and attempts to determine whether the new data protection framework provide specific data subjects' safeguards (substantive and procedural ones).

The second theory on which the research is built is the 'conceptualisation' of the right to data protection,[57] as the right of individuals to control how their personal data are used.[58]

---

[50] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Hartmut Eifert v Land Hessen* [2010] ECLI:EU:C:2010:662, para 48.
[51] Case C-291/12 *Michael Schwarz v Stadt Bochum* [2013] ECLI:EU:C:2013:670, para 33.
[52] ibid para 48.
[53] Joined Cases *Volker and Eifer*t (n 50).
[54] Jeanne Mifsud Bonnici, 'Exploring the Non-Absolute Nature of the Right to Data Protection' (2014) 28(2) International Review of Law, Computers and Technology 131, 132.
[55] e.g. *Opinion 1/15 of the Court (Grand Chamber) on the Draft Agreement between Canada and the European Union* [2017] ECLI:EU:C:2016:656, para 150.
[56] Recital 4 GDPR provides that '[t]he right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.'
[57] To borrow the expression from Tzanou in Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so New Right' (2013) 3(2) International Data Privacy Law 88, 89-90; see also Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 214-215.
[58] Formulated as a 'right to self-determination' by the German Constitutional Court in its 'Population Census Decision', the concept is however not present in all EU Member States jurisdictions, see Orla Lynskey, 'The Role of Individual Control over Personal Data in EU Data Protection Law', *the Foundations of EU Data Protection Law* (OUP 2015), 178; see Maria Tzanou, 'Data Protection as a Fundamental Right', *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing 2017) 7-44.

This concept of *individuals' control* is expressly recognised in Recital 7 GDPR.[59] Recitals 51 and 61 of the 'police' Directive also refer to the notion of control, but more in terms of 'loss of control' or 'deprivation from exercising control' resulting from risks to data subjects' rights and freedoms or from damage linked to a data breach. In Member States' traditions, and in particular in Germany, the right to control over personal data is recognised as an informational right to self-determination. However, it has never been formulated as such by the ECJ. Several authors have written about the existence and scope of such a right, at national and EU levels.[60] But as observed by Lynskey, ultimately, this control 'at best enables individuals to exercise rights' but is not absolute control over their personal data.[61] It is on this conception of relative control that the research is developed.

### *b. The Concept of 'Law Enforcement'*

The A29WP and the EDPS have criticised the reprocessing of personal data for purposes other than their original purpose of collection, and in particular, in the context of law enforcement reprocessing.[62] Some authors have conceptualised it as a 'shift in the purpose of processing.'[63] Not only have the personal data at stake been initially collected for non-law enforcement purposes (e.g. commercial purposes, operational purposes or border control purposes), but they might also relate to non-suspect individuals. As pointed out by Boehm, 'this shift ...has serious consequences for the rights of individuals, which implicitly leads to a change in the applicable data protection rights and their connected procedural guarantees.'[64] The research is built on this hypothesis. And, as data protection rules are split into two instruments – a general instrument and a specific one on law enforcement processing- it is critical to making this assessment.

In the context of this study, the term 'law enforcement' refers to both the field covered by Directive 2016/680 and the competent authorities processing the personal data within the scope of the Directive.

Following Article 1(1) of Directive 2016/680, *law enforcement purposes* are defined as 'the prevention, investigation, detection or prosecution of criminal offences or the execution of

[59] Recital 7 GDPR provides that '[n]atural persons should have control of their own personal data.'
[60] For a selected literature on the right to self-determination in Germany, see in particular, Joe Cannataci, 'Lex Personalitis & Technology-driven Law' (2008) 5(1) Scripted, 3; Gerrit Hornung and Christoph Schnabel, 'Data Protection in Germany I: the Population Census Decision and the Right to Informational Self-Determination' (2009) 25 (1) Computer Law and Review 84; Antoinette Rouvroy and Yves Poullet, 'the Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth et al (eds), *Reinventing Data Protection?* (Springer 2009) 45-76; J.C. Buitelaar, 'Privacy: Back to the Roots' (2012) 13(3) German Law Journal 171; Christophe Lazaro and Daniel Le Métayer 'The Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12(1) SCRIPT-ed 3; and at EU level, see Lynskey, 'The Link between Data Protection and Privacy in the EU Legal Order' (n 58) 89-130, and Tzanou (n 57) 40.
[61] See Lynskey, 'The Limits of Individual Control over Personal Data' (n 58) 230.
[62] As explained in Section I.
[63] Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level* (Springer 2012) 382.
[64] ibid.

criminal penalties.'[65] National security services are excluded from the scope of the Directive, as well as data processing in the area of Common Foreign and Security Policy.[66] Among the law enforcement purposes covered by the Directive, two are of particular interest due to their impact on data subjects' rights: processing for criminal surveillance and criminal investigation purposes. 'Criminal surveillance' is understood, for the purpose of this research, as surveillance led by law enforcement (or police) authorities, excluding from its scope surveillance by national security or military agencies. Criminal surveillance is not linked to a specific offence, but to 'risks and threats to security.'[67] It is used to anticipate or prevent criminal offences. As observed by Vervaele, 'in some countries these investigations [carried out in the context of criminal surveillance] are submitted to an ex-ante judicial review, in others they are not.'[68] Thus, the rules applicable to criminal intelligence might greatly vary from one Member State to another. In the absence of offences, suspects, or victims, the impacts on data subjects' rights might also be higher than those in the context of criminal investigation. By contrast, criminal investigation usually starts with an offence and falls within the criminal procedural framework at national level. However, the distinction between the two is not always clear-cut: in particular, criminal surveillance can also be used in the context of criminal investigation and target specific individuals.[69]

As for *law enforcement authorities*, those are the 'competent authorities' to whom the rules of the Directive apply. As set out in Article 3 of Directive 2016/680, they are either public authorities (police or judicial authorities) or bodies entrusted with a law enforcement task.[70] Law enforcement authorities cover both police and criminal justice authorities.

#### *c. The Notion of 'Biometric Data'*

The research investigates the notion of 'biometric data'. Until the adoption of the new data protection framework, the notion had not been officially introduced in any EU data protection legislation. The A29WP attempted to define the notion,[71] and both the EDPS[72]

[65] art 1(1) Directive 2016/680; in the USA, the concept of 'law enforcement' has a broader meaning as it also covers border enforcement, public security, national security, as well as non-criminal judicial and administrative proceedings, see Final Report by EU-US High-Level Contact Group on Information Sharing and Privacy and Personal Data Protection, 28 May 2008, 9831/08; as cited by de Busser in Els De Busser, *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities* (Maklu 2009) 401.
[66] Recital 14 Directive 2016/680.
[67] John Vervaele, 'Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reloading Data Protection* (Springer 2014) 115-116.
[68] ibid.
[69] On this specific issue, see Ira Rubinstein, Gregory Nojeim, and Ronald Lee, 'Systematic Government Access to Private-Sector Data, A Comparative Analysis' in Fred Cate and James Dempsey (eds), *Bulk Collection, Systematic Government's Access to Private Sector Data* (OUP 2017) 38-42.
[70] art 3(7)(a)-(b) Directive 2016/680.
[71] A29WP, 'Opinion 4/2007 on the concept of personal data' [2007] WP136, 8.
[72] eg EDPS, 'Opinion of the European Data Protection Supervisor on the draft Council Regulation (EC) laying down the form of the laissez-passer to be issued to members and servants of the institutions' [2006] OJ C313/36, 37 stating that: 'biometric data are sensitive by definition'; and more recently, EDPS, 'Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-

and the Court of Justice referred to their sensitive nature.[73] However, many uncertainties remained concerning the notion and the regime of data protection applicable thereof. The topic of biometrics through the lens of EU data protection and privacy has been researched in depth by Els Kindt. In the pre-GDPR area, Kindt has investigated the concept of biometric data and suggested the application of a test of proportionality for the processing of biometric data by private parties. Her work is the most comprehensive and detailed study that can be found in the field.[74] The study of Nancy Yue Liu can also be mentioned, as Liu has addressed the use of biometric technologies and compared the legal frameworks applicable in Europe, Australia, and the United States.[75] But neither study thoroughly covers the issue of law enforcement access to and use of biometric data collected by the private sector.[76]

The statutory notion of 'biometric data' is addressed in detail in Chapter 3 of the dissertation.

### *d. The Concept of 'Safeguards'*

The research aims to assess the safeguards attached to or deriving from the fundamental right to data protection. The term 'safeguards' is used in many documents relating to data protection, but it does not always refer to the same types of guarantees. Safeguards can mean the data protection principles applicable to the processing of personal data,[77] but it can also refer to data subjects' rights or the measures put in place to protect the data themselves and ensure their security or restrict access to them.[78] The term is indeed very broad. In the context of this research, 'safeguard' is understood as 'guarantee' afforded to individuals when their personal data, namely biometric data, are collected for a GDPR purpose and re-used for one of the purposes of the 'police' Directive. The research

scale information systems' [2018] 11, where the EDPS states that '…biometric data which are, by nature, very sensitive. Indeed, unlike other personal data, biometric data are neither given by a third party nor chosen by the individual; they are immanent to the body itself and refer uniquely and permanently to a person.' <https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf> accessed 30 September 2018.

[73] The ECJ did not rule that biometric data are sensitive data; but AG Mengozzi did in his Opinion in Case C-291/12, see C-291/12 *Michael Schwarz v Stadt Bochum* [2013], Opinion of Advocate General Mengozzi, para 52, EU:C:2013:401.

[74] Els Kindt, *Privacy and Data Protection Issues of Biometric Applications, A Comparative Legal Analysis* (Springer 2013).

[75] Nancy Yue Liu, *Bio-Privacy, Privacy Regulations and the Challenges of Biometrics* (Routledge 2012).

[76] Even if Els Kindt mentions the topic in her research, see Kindt (n 74) 787-790.

[77] As defined in art 5 GDPR and art 4(1) Directive 2016/680.

[78] In that sense see for instance, William Lowrance, 'Privacy, Confidentiality, Safeguards,' *Privacy, Confidentiality, and Health Research* (Cambridge University Press 2012) 34; EDPS, 'Opinion on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final)' [2005] OJ C181/13; A29WP, 'Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC' [2006] WP 119, 2-3; see also Bignami using the term to cover both safeguards to individuals and to the protection of data in Francesca Bignami, 'The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens' (Study for the LIBE Committee, European Parliament 2015) <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf > accessed 30 September 2018.

investigates, in particular, the existence of any procedural and substantive safeguards, as well as the role played by the principle of purpose limitation.

The notion of 'safeguards' originates from the ECtHR's interpretation of the right to privacy enshrined in Article 8 of the European Convention on Human Rights (ECHR) and particularly on the limitations to that right (Article 8(2) ECHR). In the interpretation of that provision, the ECtHR has checked at several occasions whether the national legislation at stake provided 'appropriate safeguards' against abuses: in particular in cases of state surveillance,[79] police surveillance,[80] or criminal cases.[81] The ECJ has further developed the notion in its judgments on data retention in the application of both Articles 7 and 8 of the Charter. It is thus relevant to assess whether the GDPR and the 'police' Directive provide appropriate safeguards to individuals when their personal data collected by private parties are reprocessed for a law enforcement purpose.[82] The research aims to define the scope and nature of these safeguards, taking into account possible limitations for the sake of criminal investigation or crime prevention. These safeguards are analysed and discussed in different chapters of the study.

## 2. Legal Framework

The legal framework applicable to the research is composed of EU primary sources, namely Articles 7 and 8 of the Charter, EU secondary legislation and more specifically the GDPR and the 'police' Directive (Directive 2016/680), and finally case law and 'soft' law instruments composed of Opinions, Guidelines and Recommendations of both the A29WP and the EDPS.

### *a. EU Primary Sources*

***Articles 7 and 8 of the Charter: fundamental rights to privacy and data protection***

In the Charter of Fundamental Rights, the right to data protection is established as a right distinct from the right to privacy. These fundamental rights are enshrined in Article 7 (*right to respect for private and family life*) and Article 8 (*right to the protection of personal data*) of the Charter.[83] While Article 7 of the Charter corresponds to Article 8 ECHR;[84]

[79] eg *Klass and others v Germany* App no 5029/71 (ECHR, 6 September 1978); *Roman Zakharov v Russia* App no 47143/06 (ECHR, 4 December 2015), and *Szabó and Vissy v Hungary* App no 37138/14 (ECHR, 12 January 2016).

[80] *Malone v the United Kingdom* App no 8691/79 (ECHR, 2 August 1984), and *Khan v UK* App no 35394/97 (ECHR, 12 May 2000).

[81] eg *M K v France* App no 19522/09 (ECHR, 18 April 2013).

[82] On this specific issue, see the report by Franziska Boehm based on the previous data protection regime, Franziska Boehm, 'A comparison between US and EU data protection legislation for law enforcement purposes' (Study for the LIBE Committee, European Parliament 2015) <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf> accessed 30 September 2018.

[83] art 7 Charter (entitled 'respect for private and family life') provides that 'everyone has the right to respect for his or her private and family life, home and communications.'

art 8 Charter (entitled 'protection of personal data') reads as follows:

a. Everyone has the right to the protection of personal data concerning him or her.

b. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified (…)

Article 8 of the Charter is based on Article 8 ECHR as well as on Article 286 of the Treaty establishing the European Community,[85] Directive 95/46/EC, and Convention 108 of the Council of Europe.[86] The Charter links the two rights but establishes them as separate rights. By contrast, the ECtHR has interpreted the right to privacy in Article 8 ECHR as encompassing the right to data protection.[87]

Although the two rights are formally distinct in the Charter, the European Court of Justice merged them into a 'hybrid' right in its case law decided just after the entry into force of the Charter. Mentioning explicitly both Articles 7 and 8 of the Charter, the Court referred to a 'right to respect for private life with regard to the processing of personal data.'[88] Some authors criticised this approach, opining that the ECJ should have instead established the existence of a fundamental right to data protection, next to the right to privacy.[89] In later decisions, the ECJ seems to have abandoned this approach, clearly distinguishing the two rights and citing Articles 7 and 8 individually.[90]

***Article 16 TFEU: Single Basis for Secondary EU Law in the Field of Data Protection***

Introduced by the Lisbon Treaty, Article 16 of the Treaty on the Functioning of the EU is the horizontal legal basis on which EU legislation on data protection across sectors is adopted.[91] It sets up the ordinary legislative procedure to adopt data protection rules applicable to different policy areas, including internal market and law enforcement. It is on this ground that the EU institutions have adopted both the GDPR and the 'police' Directive. However, despite the collapse of the pillar structure, Article 16 TFEU does not imply that data protection rules will apply across all sectors via the same instrument. Rules on data processing in the area of Common Foreign and Security Protection remain subject to a different legal basis.[92] As for law enforcement processing, Declaration 21 of the Lisbon Treaty acknowledges their 'specific nature',[93] allowing for the adoption of a

c. Compliance with these rules shall be subject to control by an independent authority.

[84] As acknowledged in the Explanations relating to the Charter of Fundamental Rights (n 49) 20.

[85] Replaced by Article 16 TFEU and Article 39 TEU.

[86] See Explanations relating to the Charter (n 49) 20.

[87] In particular, *S and Marper v the United Kingdom* App nos 30562/04 and 30566/04 (ECHR, 4 December 2008), para 103: '[t]he protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention.'

[88] *Volker and Eifert (*n 50) para 52.

[89] eg Tzanou (n 57) 88-99; González Fuster (n 57) 234-235; but note, in contrast, Lynskey's analysis who observed that it was too early to draw conclusions and that in the end the Court might not consider 'data protection as a subset of the right to privacy' in Orla Lynskey, 'Reconciling Data Protection with Other Rights and Interests' (n 58) 174.

[90] eg Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and others* [2016] ECLI:EU:C:2016:970, and Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.

[91] To the exclusion of the Common Foreign and Policy Security Matters.

[92] Following art 39 Treaty on European Union.

[93] 'Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation', No. 21, Declarations Annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, OJ EU C 83/335, 345.

different data protection regime in that area.[94] As a consequence, the data protection package was not proposed as an 'overarching' instrument, but instead as a *lex generalis* (the GDPR) completed by a *lex specialis* for law enforcement processing (the 'police' Directive).

### *b. EU Secondary Legislation*

Before the entry into force of the Lisbon Treaty, the EU competences were split into three pillars: the first pillar covering internal market matters, the second foreign and security matters, while the third on freedom, security and justice included criminal and police cooperation matters.

#### *Pre-Lisbon Treaty*

The main text applicable to the processing of personal data for internal market issues was the Data Protection Directive (Directive 95/46/EC);[95] while a patchwork of rules applied to third pillar matters.[96] For instance, several ad hoc Council Framework Decisions were adopted in the areas of security, police cooperation, and police and judicial cooperation agencies.[97] But the most relevant instrument for law enforcement processing was the Council Framework Decision 2008/977/JHA on the protection of personal data processed by law enforcement authorities.[98] The scope of this instrument was, however, limited to cross-border data processing.[99] Member States were also encouraged to take into account the non-binding Council of Europe's Recommendation on the use of personal data in the police sector (Recommendation R(87)15).[100] The application of the Recommendation has also led to many discrepancies at the national level, as established in the report 'Recommendation R(87)15: Twenty-Five Years Down the Line.'[101]

---

[94] As analysed by Lynskey in Orla Lynskey, 'The Key Characteristics of the EU Data Protection Regime' (n 58) 19; despite the statement made by the EU Commission in European Commission 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee of the Regions: A Comprehensive Approach to Personal Data Protection in the European Union' COM (2010) 609 final [2010] 4: 'In particular, the new legal basis allows the EU to have a single legal instrument for regulating data protection, including the areas of police cooperation and judicial cooperation in criminal matters.'

[95] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of such data (Directive 95/46/EC) [1995] OJ L281/31.

[96] See among others, Hielke Hijmans and Alfonso Scirocco, 'Shortcomings in EU Data Protection in the Third and Second pillars. Can the Lisbon Treaty Be Expected to Help?' 46(5) Common Market Law Review 1485, 1496-1497.

[97] For more detailed analysis, see Paul De Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) 7(1) New Journal of European Criminal Law 7.

[98] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Council Framework Decision 2008/977/JHA) [2008] OJ L350/60.

[99] Recital 7 Council Framework Decision 2008/977/JHA.

[100] Council of Europe Recommendation No R(87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector [1987] <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e7a3c> accessed 30 September 2018.

[101] Joseph A Cannataci and Mireille M Caruana, 'Recommendation R(87) 15: Twenty-Five Years Down the Line' (2013) Report to the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, T-PD(2013) 11

***New Data Protection Framework***

After the entry into force of the Lisbon Treaty, the European Commission proposed in 2012 a complete overhaul of the data protection rules. The European Commission initially planned to introduce a single instrument to regulate data processing, including in the police and criminal justice area.[102] However, as noted by Lynskey,[103] instead of proposing a 'comprehensive instrument,' the European Commission proposed two distinct instruments: a general regulation, which became the General Data Protection Regulation (GDPR),[104] and a specific Directive, which became the 'police' Directive applicable to domestic and cross-border processing of personal data in the law enforcement area.[105] The GDPR has repealed Directive 95/46/EC, and the 'police' Directive has replaced the Council Framework Directive 2008/977/JHA while extending its scope to domestic data processing.[106]

### *c. Case Law and Soft-Law Instruments*

The research builds on a review of the ECtHR and the ECJ's respective case law relating to the processing of biometric data,[107] the test of necessity and proportionality (including as applied in the context of surveillance),[108] as well as the retention of data and their access for law enforcement purposes.[109]

Besides, the research relies on opinions, recommendations, or guidelines, issued by both the A29WP and the EDPS. In particular, the A29WP has adopted several documents relevant to biometric data and biometric technologies pre-GDPR area. Both the A29WP and the EDPS have adopted opinions on the new data protection framework. As a side note, it should be observed that the European Data Protection Board, which replaces the A29WP, has endorsed A29WP documents relating to the GDPR.[110]

---

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806840b2> accessed 30 September 2018.

[102] European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee of the Regions: A Comprehensive Approach to Personal Data Protection in the European Union' COM (2010) 609 final, 4: 'In particular, the new legal basis allows the EU to have a single legal instrument for regulating data protection, including the areas of police cooperation and judicial cooperation in criminal matters.'
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2010:0609:FIN> accessed 30 September 2018.

[103] Lynskey (n 94).

[104] GDPR (n 22).

[105] Directive 2016/680 (n 23).

[106] See respectively Recital 7 Council Framework Decision 2008/977/JHA, and Recitals 6 and 7 Directive 2016/680.

[107] eg *S and Marper v United Kingdom* (n 87); *Michael Schwarz v Stadt Bochum* (n 51); Joined Cases C-446/12 to V-449/12 *WP Willems and others* [2015] ECLI:EU:C:2015:238.

[108] eg *Handyside v UK App* no 5493/73 (ECHR, 7 December 1976); *Digital Rights Ireland* (n 90); *Tele2 Sverige* (n 90), and *Schrems* (n 90).

[109] In particular *Digital Rights Ireland* (n 90) and *Tele2 Sverige* (n 90).

[110] See the list in EDPB, 'Endorsement 1/2018' [2018]
<https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf> accessed 30 September 2018.

## V. Structure

The thesis is composed of seven chapters, including the introduction and the conclusion. Four of the chapters are comprised of articles published in peer-reviewed journals. Each of them has tackled one of the issues raised by the topic. The journals in which parts of the thesis have been published are the International Data Privacy Law Journal (Oxford), the Computer Law and Security Review (Elsevier), and the European Data Protection Law Review (Lexxion). The journals were selected for the audience they reach, their rankings, as well as their specific scope. Two of them focus on data protection and privacy issues, whereas one covers legal and technological topics. The articles are reproduced as published, save three minor modifications. First, for consistency with the other chapters, the headings and sub-headings of the first article have been aligned with the structure of the other articles. Second, in the third article (chapter 4), the term 'data' was initially used as a singular noun due to editorial requirements. However, as 'data' is used in all the other chapters as a plural noun, the third article has been amended accordingly.[111] Last, for better readability, the footnotes of the different articles have been harmonised as much as possible.

***Chapter 1*** introduces the research and sets out the background, the research questions, the methodology followed, as well as the theoretical framework. As a preliminary remark, it should be acknowledged that the research started in 2014 under the previous EU data protection regime, composed of the Data Protection Directive and a patchwork of rules applicable to law enforcement authorities for the processing of personal data. In the course of the research, the new EU data protection reform package was adopted. The adoption of the new regulatory framework implied to shift the focus of the study to the interpretation of the new provisions.

***Chapter 2*** addresses several terminological issues. It builds on an observation: the lack of rigour from EU bodies and institutions when they use the term 'biometrics' to mean interchangeably 'biometric methods', 'automated recognition' or 'biometric data.' From this observation was born the need to clarify and distinguish the concepts of 'biometrics' and 'biometric data' from both a technological and a legal perspective. The article has surveyed reports, opinions, and other documents published by European bodies and institutions. It looks at the differences between legal and technological realities. Written before the adoption of the new EU data protection framework, it extends the analysis to the European sphere covering both the EU's and the Council of Europe's legal orders. Published in the International Data Privacy Law, the article is entitled ***'Avoiding Terminological Confusion between the Notions of 'Biometrics' and 'Biometric Data': an***

[111] It should be noted that both forms can be used and the choice to use the term 'data '(eg personal, sensitive or biometric data) as a plural noun was guided by its usage by the EU institutions in the legal instruments of reference.

***Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective.'***

Building on the previous chapter, ***Chapter 3*** analyses the legal nature of biometric data after the adoption of the new EU data protection framework. It focuses on the statutory definition of 'biometric data'. The article is one of the early interpretations of the definition. The article describes the four components of the definition and addresses, in particular, the issue of identification from both data protection and technological perspectives. It finds out that the concepts do not match, as the concept of biometric identification is very narrow and specific. It also criticises the criterion used to classify biometric data as a type of sensitive data: according to the GDPR, they are not sensitive per nature but become sensitive if they are processed to *uniquely identify* an individual. By contrast, genetic data that also relate to individuals' unique attributes are sensitive by nature. Based on the state-of-the-art in biometric recognition, which allows the disclosure of a vast amount of information about an individual (including his or her kinship),[112] the article questions whether the distinction made between genetic data and biometric data is justified and sustainable. Entitled '***Legal Nature of Biometric Data: from 'Generic' Personal Data to Sensitive Data***,' the article is published in the European Data Protection Law Review.

Having set the legal and technical background, ***Chapter 4*** and ***Chapter 5*** analyse the scenario of law enforcement access to and re-use of personal data collected by the private sector. The two chapters raise the issue of the interface between the GDPR and Directive 2016/680. While the GDPR applies to the collection of personal data by private parties, the rules contained in Directive 2016/680 apply to the subsequent use of these data for a law enforcement purpose. Chapters 4 and 5 are not specific to the processing of biometric data but are illustrated with cases involving the processing of biometric data.

***Chapter 4*** reproduces the article published in the Computer Law and Security Review journal under the title '***Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?'*** The purpose of the article is to determine whether Directive 2016/680 provides adequate safeguards when personal data originating from the private sector are further accessed and used by law enforcement authorities. The article builds on the findings of the ECJ's case on data retention, and more specifically *Digital Rights Ireland* and *Tele2 Sverige*. The scenarios at the origin of the Court's decisions are different since in the two cases data are mandatorily retained by private parties to be later accessed and used by law enforcement authorities. However, the article applies the findings by analogy and finds out that Directive 2016/680 might not provide adequate procedural and substantive safeguards.

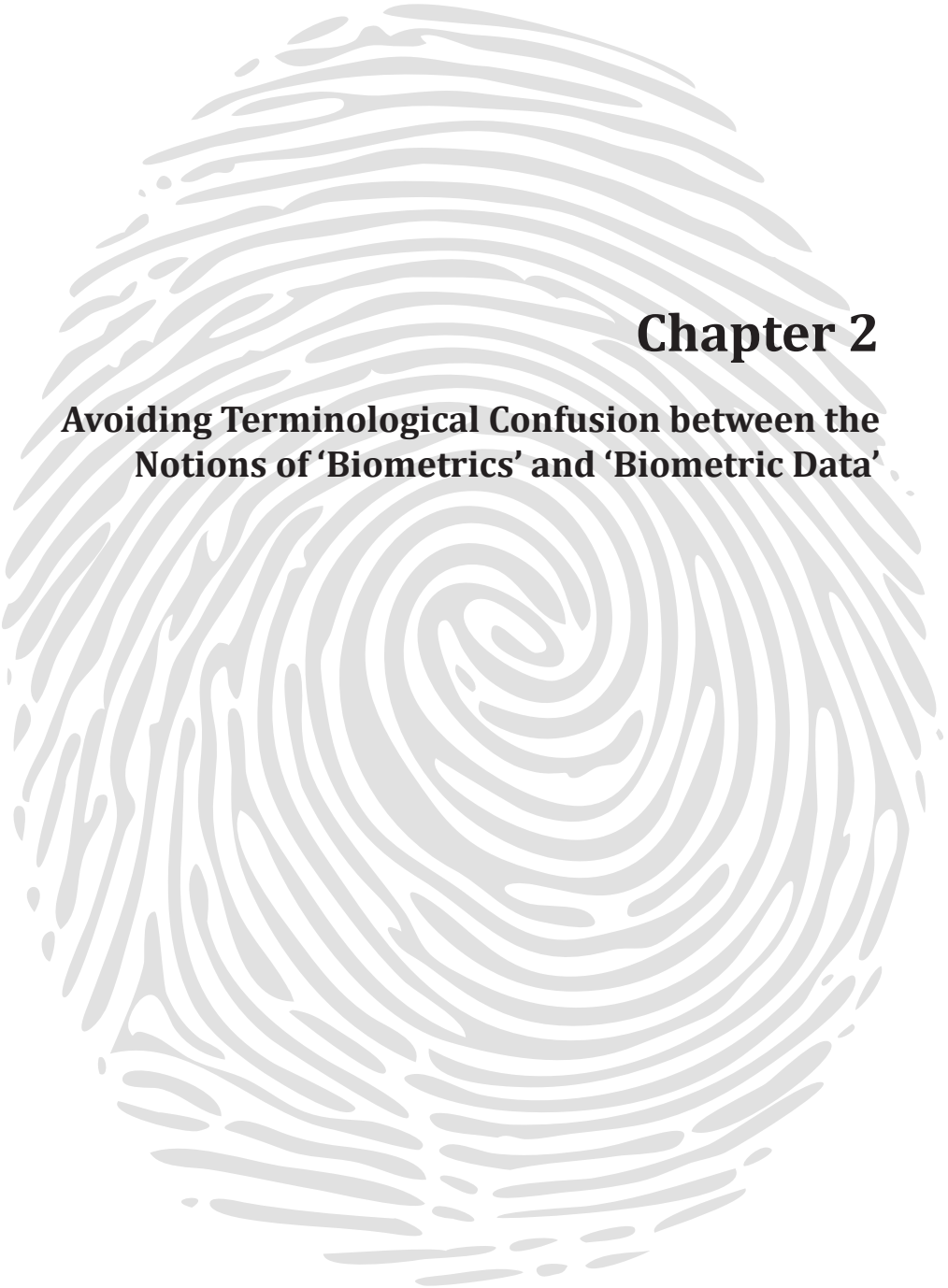
[112] There is very recent research on this issue in the area of face verification; see for instance Miguel Bordallo Lopez et al, 'Kinship Verification from Facial Images and Videos: Human versus Machine' (2018) 29(5) Machine Vision and Applications 873.

In particular, the right to information defined in Article 13 of the Directive, does not impose an obligation to inform and notify individuals that law enforcement authorities have further processed their personal data. If law enforcement purposes may justify a delay in providing the information to an individual, they do not justify an absence of notification. This notification is crucial for individuals, as it will trigger their right to remedy, as well as other data subjects' rights. Last, the article briefly touches upon the issue of the principle of purpose limitation as a safeguard in reprocessing data across the two instruments. This last issue makes a transition to the next chapter, which is entirely dedicated to that principle.

***Chapter 5*** questions the role played by the principle of purpose limitation when processing operations are carried out across the two instruments. Published in the European Data Protection Law Review, the article focuses on the '***Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?***' The principle of purpose limitation seems to be an essential element, as it is explicitly mentioned as one of the components of the fundamental right to data protection (Article 8 of the Charter). Reviewing the rules established respectively in the GDPR and Directive 2016/680, the scenario of subsequent processing across the two instruments seems to be forgotten or voluntarily omitted. Building on the ambiguous wording of Article 4(2) of Directive 2016/680, the article suggests a bold interpretation to find a role for the principle of purpose limitation. However, aware that this interpretation might not be dominant, the article concludes on the likelihood of diverging interpretations among Member States. This issue illustrates the existence of shortcomings in the relationship between the two instruments.

***Chapter 6*** provides some recommendations to mitigate the risks to individuals' right to data protection based on the Data Protection by Design and the Data Protection Impact Assessment measures. A part of the chapter is built on a conference paper discussing the relationship between the concept of 'Privacy by Design' and the principle of purpose limitation. Although as yet unpublished, the chapter is added to the dissertation to provide some recommendations tailor-made to the law enforcement use of biometric data generated by the private sector. It is intended to submit this chapter for publication.

Finally, ***Chapter 7*** summarises the key findings of the study, answers the research question, and suggests paths for future research in the field. It suggests focusing, for instance, on case studies, such as facial recognition.



# Chapter 2

## Avoiding Terminological Confusion between the Notions of 'Biometrics' and 'Biometric Data'

## *Chapter 2: Avoiding Terminological Confusion between the Notions of 'Biometrics' and 'Biometric Data'*

*An Investigation into the Meanings of the Terms from a European Data Protection and a Scientific Perspective**

**Abstract:**
*This article has been motivated by an observation: the lack of rigour by European bodies when they use scientific terms to address data protection and privacy issues raised by biometric technologies and biometric data. In particular, they improperly use the term 'biometrics' to mean at the same time 'biometric data', 'identification method', or 'biometric technologies.' Based on this observation, there is a need to clarify what 'biometrics' means for the biometric community, and whether and how the legal community should use the term in a data protection and privacy context. In parallel to that exercise of clarification, there is also a need to investigate the current legal definition of 'biometric data' as framed by European bodies at the level of the European Union and the Council of Europe. The comparison of the regulatory and scientific definitions of the term 'biometric data' reveals that the term is used in two different contexts. However, it is legitimate to question the role that the scientific definition could exercise on the regulatory definition. More precisely, the question is whether the technical process through which biometric information is extracted and transformed into a biometric template should be reflected in the regulatory definition of the term.*

### I. Introduction

Biometric technologies allow the capture, collection, and processing of biometric information about individuals. Their information is then transformed into digital bits that can be retrieved when necessary for comparison. The biometric processing of individuals' information and data raises personal data protection issues. The first one is whether individuals' biometric data constitute a category of personal data as defined at European level. But to be able to determine the legal regime applicable to biometric data, one must understand and assess the definition(s) given to the term 'biometric data' by the European data protection community. This is highly relevant since the European Commission has introduced a regulatory definition of the term in its proposals of revision of the European

* Article published in the International Data Privacy Law journal (IDPL), volume 6, issue 1, February 2016, pages 63-76; the author wishes to thank Prof Jeanne Mifsud Bonnici and Prof Laurence Gormley for their very valuable comments and the anonymous peer-reviewers. The views expressed in this article are solely those of the author. All remaining errors are the author's sole responsibility.

Data Protection Framework. This reform, commonly designated under the name of the Data Protection Reform Package,[1] is composed of a General Data Protection Regulation (GDPR) (replacing the current Data Protection Directive, Directive 95/46/EC)[2] and a specific Directive on data protection and law enforcement (replacing the current Council Framework Decision 2008/780/JHA).[3] The European Parliament (EP) voted in first reading the two proposals of the package in March 2014,[4] whereas the Council of the European Union (EU) only agreed in June 2015 on a text for the GDPR.[5] At the time of writing, the European Commission, EP and Council of the EU have started a 'trilogue' on the proposal of the GDPR,[6] whereas the Council of the EU pursues its discussions among its members on the proposal for a Directive in law enforcement and data protection. As a consequence, regulatory definition of biometric data at EU level referred to in the article is the one contained in the original proposal of the GDPR together with its amended version adopted by the European Parliament and agreed by the Council of the EU.

By clarifying the meaning of 'biometric data' from a European data protection perspective, there is a need to distinguish it from the term 'biometrics'. As will be explained in the first section 'Biometrics: a catchall notion?', different European bodies have indeed used the term 'biometrics' in their legal opinions and reports to mean all at the same time

[1] The two proposals are designated under the expression 'Data Protection Reform Package', although it is not the official name given by the European Commission. However, several European bodies, such as the European Data Protection Supervisor, have used this expression to designate the two proposals. See, for example, EDPS 'Opinion of the European Data Protection Supervisor on the data protection reform package' [2012] <https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf > accessed 20 July 2015.

[2] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final [2012] <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN> accessed 20 July 2015.

[3] European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final, 2012/0010 (COD) [2012] <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=en > accessed 20 July 2015.

[4] European Parliament, legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012) 0011- C7-0025/2012 – 2012/0011 (COD)) [2014] < http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402 > accessed 20 July 2015.
European Parliament, legislative resolution on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM (2012) 0010 – C7-0024/2012 - 2012/0010 (COD)) [2014] < http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0219 > accessed 20 July 2015.

[5] Council of the EU, proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Preparation for a general approach 9565/15 (11 June 2015) [2015] <https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf> accessed 30 August 2015.

[6] European Commission's press release: <http://europa.eu/rapid/press-release_STATEMENT-155257_fr.htm> accessed 20 July 2015.

'biometric data', 'identification method', and 'biometric technologies'.[7] This article claims that the term 'biometrics' is first a technical term that does not have any legal meaning from a data protection perspective. After having described the notion of 'biometrics', the article will focus, in the second section 'Biometric data: a technical and a legal notion', on the notion of 'biometric data', which is crucial from a data protection point of view. It will argue that the term refers to two different notions, a legal one and a scientific one, which cannot be merged into a single one since they serve different purposes. The article will explain the fundamental difference between the two and will investigate whether or not the legal definition should reflect the scientific definition.

This article focuses on terminological issues and not on the legal nature of 'biometric data'. However, defining 'biometric data' and as a consequence 'biometrics' is a necessary first step to later assess the legal nature of 'biometric data' from a European data protection perspective. This following step is not the topic of the current article but of a subsequent one. In addition, this article will attempt to bridge a gap between legal experts in the European data protection field and scientists in the biometric field. Both types of experts use the same terms but give them different meanings.[8] By understanding how scientists are approaching the two notions, this article will assess whether (and how) the regulatory definitions of 'biometrics' and 'biometric data' should reflect the scientific ones. It will however not assess whether the scientific definitions might need to reflect the legal ones.

The text of reference on the scientific side is the International Standard ISO/IEC 2382-37 harmonising the vocabulary used in the field of biometrics.[9] Although the current version of the Standard is the first one published and might be subject to revision, it has already been quoted as a document of reference by national data protection authorities.[10] The Standard contains more than 100 entries that are used in the field of biometrics. References to its definitions will mainly focus on the two most relevant notions in a data protection context: 'biometrics' and 'biometric data'. Other terms used in the field of biometrics will be mentioned in the course of this article, but they will not be thoroughly analysed. To reflect the diversity of definitions and disciplines, several scientific sources published before the adoption of the International Standard will also be mentioned. They include, among others, definitions in glossaries [the *Glossary of Biometric Terms* of 1999

[7] See for example, Article 29 Data Protection Working Party, 'Opinion 3/2012 on developments in biometric technologies' [2012] WP193.

[8] This article has been inspired by discussions with biometric experts and engineers working in the field of biometrics. Experts in different fields use the same terms with different meanings without necessarily acknowledging the differences. Concerning the term 'biometrics', it is first of all a technical term. As a consequence, on cannot ignore its meaning from a scientific perspective.

[9] ISO/IEC 2382-37: 2012 (E)—Information Technology—Vocabulary—Part 37: Biometrics <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55194> accessed 20 July 2015.

[10] Il Garante (Italian Data Protection Authority), Guidelines on Biometric Recognition and Graphometric Signature, Annex A to the Garante's Order of 12 November 2014, 3 <http://194.242.234.211/documents/10160/0/GUIDELINES+ON+BIOMETRIC+RECOGNITION> accessed 20 July 2015.

and the *Biometrics Glossary* of the US National Science and Technology Council (NSTC) of 2006],[11] a report on Biometric Recognition,[12] and the Encyclopedia of Biometrics.[13]

On the side of data protection and privacy in relation to biometric technologies, the review of the existing literature is based on two main studies. The first is *Bio-Privacy, Privacy Regulations and the Challenge of Biometrics* by Nancy Yue Liu.[14] The second is the reference work on *Privacy and Data Protection Issues of Biometric Applications* by Els Kindt.[15] In the first book, the author briefly describes the notion of 'biometrics' in a short section on terminology, whereas in the second book, the author thoroughly assesses the legal nature of biometric data and proposes her own definition. If this article is built on their research, it also goes beyond. It proposes to investigate how the scientific definitions of 'biometrics' and 'biometric data' by the biometric community can help the European data protection community to understand the notion of 'biometrics' and to determine whether the scientific definition could be used to 'reshape' the legal definition of 'biometric data'.



Legal opinions, reports, and legislative reports at the European data protection level will also be reviewed. For the purpose of this article, the European level should be understood as encompassing the level of the EU and of the Council of Europe. At both levels, several initiatives and measures addressing biometric issues are interesting to assess.

More precisely, at EU level, Opinions and a *Working Document on biometrics* issued by the Article 29 Working Party as well as different Opinions of the European Data Protection Supervisor (EDPS) on biometric issues will be surveyed. This part is completed by the analysis of the European Commission's proposals on the Data Protection Reform Package. Whenever necessary, a distinction will be made between the text proposed by the European Commission, the text adopted at first reading by the EP, and the text agreed by the Council of the EU.

Besides initiatives at the EU level, several documents adopted at the level of the Council of Europe on biometric issues deserve special attention. First of all, the issue of the application of the principles contained in Convention 108 to biometric data was raised in 2005 in a Progress Report drafted by the Consultative Committee of the Convention.[16] The

[11] Association for Biometrics and International Computer Security Association, '1999 Glossary of Biometric Terms,' 1-12 <biometrics3.tripod.com/pubs/glossary.pdf> accessed 20 July 2015; US National Science and Technology Council's Subcommittee on Biometrics, 'Biometrics Glossary' (2006), 1-33 <http://www.biometrics.gov/documents/glossary.pdf> accessed 20 July 2015.
[12] Whither Biometrics Committee & National Research Council, *Biometric Recognition: Challenges and Opportunities*, JN Pato and LI Millett (eds) (The National Academies Press 2010).
[13] Stan Z Li (ed), *Encyclopedia of Biometrics* (1st edn, Springer 2009).
[14] Nancy Yue Liu, *Bio-Privacy, Privacy Regulations and the Challenge of Biometrics* (Routledge 2012).
[15] Els Kindt, *Privacy and Data Protection Issues of Biometric Applications, A Comparative Legal Analysis* (Springer 2013).
[16] Council of Europe, Consultative Committee of Convention 108, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' (2005) <http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Biometrics_2005_en.pdf > accessed 20

Parliamentary Assembly of the Council of Europe (PACE) also raised in 2011 the importance to take into account 'the human rights implications of biometrics' through notably a standardised definition of 'biometric data'. For this reason, three documents, Resolution 1797 (2011), Recommendation 1960 (2011), and the preparatory report of the Resolution and Recommendation, called the Haibach Report, have been analysed.[17] Last but not least, the draft explanatory report on the modernisation of Convention 108 is also mentioned.[18]

## II. 'Biometrics': A Catchall Notion?

In a general dictionary, such as Merriam-Webster, the term 'biometrics' is defined in two different ways. It is a synonym of 'biometry', understood as 'the statistical analysis of biological observations and phenomena'.[19] It also means 'measurement and analysis of unique physical or behavioural characteristics (as fingerprints or voice patterns) especially as a means of verifying identity'.[20] For scientists from different disciplines (such as medicine, mathematics, statistics, or biometrics),[21] the term has more than two meanings. These multiple meanings have indeed created the need to harmonise the vocabulary used in the biometric field. In the field of data protection and privacy, the different European institutions and bodies that have assessed biometric issues have not always used the term 'biometrics' in a consistent way.

Ultimately, in conclusion of the section, the article will determine whether or not the term 'biometrics' should be used in a data protection and privacy context.

July 2015. The report was updated in 2013 by an academic report, which has not been analysed in the article since it has not been issued nor endorsed by the Council of Europe or any of its bodies.

[17] Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights, 'The Need for a Global Consideration of the Human Rights Implications of Biometrics,' Rapporteur H Haibach, Doc 12 522 (16 February 2011) <http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=13103&lang=en> accessed 20 July 2015; Parliamentary Assembly of the Council of Europe, Recommendation 1960 (2011), 'The Need for a Global Consideration of the Human Rights Implications of Biometrics' <http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=17964&lang=en> accessed 20 July 2015; Parliamentary Assembly of the Council of Europe, Resolution 1797 (2011), 'The Need for a Global Consideration of the Human Rights Implications of Biometrics' <http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=17968&lang=en> accessed 20 July 2015.

[18] Council of Europe, Bureau of the Consultative Committee of Convention 108 for the protection of individuals with regard to automatic processing of personal data [ETS. No. 108], 'Draft Explanatory Report of the Modernised Version of Convention 108' (based on the proposals adopted by the 29th Plenary meeting of the T-PD), Strasbourg, 25 March 2014, TP-PD- BUR (2013) 3ENrev5 <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR(2013)3Rev5%20-%20Draft%20explanatory%20report.pdf> accessed 20 July 2015, latest version available at the time of writing.

[19] <http://www.merriam-webster.com/dictionary/biometry> accessed 20 July 2015.

[20] <http://www.merriam-webster.com/dictionary/biometrics> accessed 20 July 2015.

[21] Stephen Stiegler, 'The Problematic Unity of Biometrics' (2000) 56 Biometrics 653.

## 1. Uses of the Term 'Biometrics' in the European Data Protection Context

Neither of the two founding legal texts on data protection and privacy at the European level mentions the term 'biometrics' or 'biometric data'.[22] These two texts are the Council of Europe's Convention 108 (Convention 108)[23] and Directive 95/46/EC on data protection (Data Protection Directive).[24] However, different European bodies have addressed the issues of the impact of the use of biometric technologies on data protection and privacy principles. All the definitions mentioned in this section are recapped in Table 1.

### *a. 'Biometrics' Used as a Synonym of 'Biometric Data'*

At EU level, the first body to analyse the notion of 'biometrics' from a data protection perspective is the Article 29 Data Protection Working Party (Working Party or Art. 29 WP).[25] Its work on biometric issues has had a major influence on other European bodies, and in particular on the EDPS.

The first document published by the Article 29 Data Protection Working Party is a *working document on biometrics* in 2003,[26] followed in 2012 by Opinion 3/2012 on the *recent developments in biometric technologies.*[27] In the working document, the Working Party assessed whether and how the Data Protection Directive could apply to the processing of biometric data. The term 'biometrics' is used throughout the report without being expressly defined. But one understands that the word is constantly used as a synonym of 'biometric data'.[28] A textual analysis of Opinion 3/2012 reveals that the term 'biometrics' is also used as a synonym of 'biometric data',[29] however not in a consistent way. In several paragraphs of the Opinion, the Working Party used the term 'biometrics' to also mean 'identification method'[30] and 'biometric technologies'[31]. But at no point did the Working

[22] Data protection and privacy as 'separate concepts'; see, for example, Peter Hustinx, 'European Leadership in Privacy and Data Protection' in Artemi Rallo Lombarte and Rosario García Mahamut (eds), *Hacia un Nuevo Derecho European de Protección de Datos, Towards a New European Data Protection Regime* (Tirant lo Blanch 2015) 15-25.

[23] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981 (ETS No. 108) <http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm> accessed 20 July 2015.

[24] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[25] The Working Party is an independent advisory body to the European Commission on data protection matters; for the composition and description of the Article 29 Working Party, see <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm> accessed 20 July 2015.

[26] A29WP, 'Working Document on biometrics' [2003] WP80.

[27] A29WP, Opinion 3/2012 (n 7).

[28] A29WP, Working Document on biometrics (n 26); see, for example, the following sentences as illustration: 'This kind of data [referring to biometrics] is of special nature' (p.2); 'There are discussions concerning the incorporation of biometrics on ID cards, passports, travel documents and visa,' p. 2, fn 2.

[29] See, for example, in Opinion 3/2012 (n 7), the use of 'biometrics' in the following sentences: 'collecting different biometrics' (p.6), 'to use biometrics of an employee', (p.11) (…) 'biometrics must not be taken from somebody without his knowledge' (p.14).

[30] A29WP, Opinion 3/2012 (n 7); see, for example; the use of 'biometrics' in the following sentence: 'Biometrics are, in some cases, replacing or enhancing conventional identification methods', p.16.

[31] A29WP, Opinion 3/2012 (n 7); see, for example, the use of 'biometrics' in the following sentences: 'new trends on biometrics', p.16, title of Section 4.2 of the Opinion that describes new biometric technologies; 'multi-modal biometrics (…) can be defined as the combination of different biometric technologies to enhance the accuracy or performance of the system', p.6.

Party specify using different meanings of the term. Besides these few paragraphs, the Working Party seems to have consistently and constantly used the term 'biometrics' as a synonym of 'biometric data'.[32] The notion of 'biometric data' has not been defined by the Working Party in its Opinions addressing biometric issues but in Opinion 4/2007 on the general *concept of personal data.*[33] This definition will be reviewed in the section 'Biometric data: a technical and a legal notion'.

In its own Opinions relating to biometric issues,[34] the EDPS has used the term 'biometrics' as a synonym of 'biometric data' and has referred to the definition elaborated by the Article 29 Data Protection Working Party in Opinion 4/2007.[35] However, as explained in the following sub-section, the glossary of the EDPS, available on its website, contains a definition of 'biometrics', which is not in line with the Working Party's definition.

Finally, it should be mentioned that the term 'biometrics' is not mentioned in the Data Protection Reform Package. The term appears, however, in the impact assessment document of the proposals, in which it is used as a synonym of 'biometric data'.[36] But no further detail on its meaning or origin is provided.

[32] For example, A29WP, 'Opinion No 7/2004 on the inclusion of biometric elements in the residence permits and visa taking account of the establishment of the European information system on visas (VIS)' [2004] WP 96, and A29WP, 'Opinion 3/2005 on implementing the Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travelled documents issued by Member States' [2005] WP112.

[33] A29WP, 'Opinion 4/2007 on the concept of personal data' [2007] WP136.

[34] See, for example, EDPS, 'Opinion the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final)' [2005] OJ C181/13.
EDPS, 'Opinion on the Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II) (COM (2005) 230 final)'; the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II) (COM (2005) 236 final) and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM (2005) 237 final)' [2005] OJ C91/38.
EDPS, 'Opinion of the European Data Protection Supervisor on the modified proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals' [2006] OJ C320/21.
EDPS, 'Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States' [2008] OJ C200/1.

[35] See paragraph 18 of EDPS, Opinion on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs) [2011]
<https://edps.europa.eu/sites/edp/files/publication/11-02-01_fp7_en.pdf> accessed 20 July 2015.

[36] See the following sentence: 'including biometrics amongst the sensitive data' (p.115) in European Commission, 'Impact Assessment accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' SEC (2012) 72 final [2012]
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=en> accessed 20 July 2015.

### *b. 'Biometrics' Used as a Synonym of 'Biometric Technologies'*

Several bodies belonging to the Council of Europe's level have used the term 'biometrics' as synonyms of 'biometric technologies' or 'biometric systems' in the specific context of personal data and in the broader context of human rights. In addition, the EDPS and to some extent the Article 29 Data Protection Working Party have also used the term 'biometrics' in that sense.



At the Council of Europe's level, the Consultative Committee of Convention 108, in charge of monitoring the implementation of the principles contained in the Convention, has been the first to define the term 'biometrics'. In a progress report *on the application of the principles of Convention 108 to the collection and processing of biometric data,*[37] it has defined the term as: '(s)ystems that use measurable, physical or physiological characteristics or personal behaviour traits to recognize the identity or verify the claimed identity of an individual'.[38]

The PACE has reused the definition of the Consultative Committee when it tackled the issue of *the human rights implications of biometrics* in Resolution 1797 and Recommendation 1960.[39] But the preparatory report of these two instruments inaccurately mentions the glossary of the EDPS as the source of the definition instead of the progress report of the Consultative Committee.[40]

In its glossary of terms available on its website, the EDPS has indeed defined the term 'biometrics' not as 'biometric data', but as a method of recognition based on biometric characteristics (see Table 1 for the exact wording). This definition calls for several remarks. First of all, the glossary of terms is not legally binding.[41] It constitutes a compilation of definitions originating from different EU institutions. The function of the glossary is to provide readers with a better understanding of data protection issues. Second, as specified on the website, most of the definitions link to their sources. In the case of the definition of 'biometrics', no source is indicated. Third, even if it does not have any legal value, it has been quoted (even if wrongly). This indicates that it has at least a value of reference.

[37] Progress Report (n 16).
[38] Progress Report (n 16) para 16.
[39] Recommendation 1960 (2011) (n 17) and Resolution 1797 (2011) (n 17).
[40] Haibach Report (n 17).
[41] The Opinions of the EDPS are also not binding, but they constitute authoritative advice. See EDPS, 'The EDPS as an Advisor to EU Institutions on Policy and Legislations: Building on Ten Years of Experience, Policy Paper', Brussels, 6 June 2014 <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/14-06-04_PP_EDPSadvisor_EN.pdf> accessed 20 July 2015.

***Table 1: Definition of 'Biometrics' in the European Data Protection Context***

| European bodies | Definitions of 'biometrics' |
|---|---|
| **Article 29 Working Party** | 1. Mainly synonym of biometric data.<br>(Working document on biometrics, Opinion 7/2004, Opinion 3/2012)<br>2. Occasionally synonym of identification method or biometric technologies.<br>(Opinion 3/2012) |
| **EDPS** | 1. Synonym of biometric data.<br>(EDPS's various Opinions)<br>2. Methods for uniquely recognising humans based upon one or more intrinsic physical or behavioural traits.<br>(EDPS's glossary of terms) |
| **Consultative Committee of Convention 108** | Systems that use measurable, physical or physiological characteristics, or personal behaviour traits to recognize the identity or verify the claimed identity of an individual.<br>(Progress report, 2005) |
| **PACE** | Same definition as the one contained in the 2005 Progress Report.<br>(Haibach report, 2011) |

### 2. Definitions of 'Biometrics' by the Scientific Community

In science understood as a broad discipline, the term 'biometrics' has multiple meanings. According to the Encyclopedia of Biometrics, there are several explanations. Biometrics is a relatively new field. As a logical consequence, the literature in that area 'contain(s) a variety of definitions for any single biometric term, as well as a variety of terms for seemingly the same concept.'[42] Glossaries produced by several associations and national councils have added some confusion by proposing diverging definitions for the same term. To provide clarity to the biometric industry, the International Standards Organisation (ISO) together with the Electrotechnical Commission (IEC) has established a specific working group to harmonise the biometric vocabulary.[43] This has resulted in the publication, in December 2012, of the first version of the ISO/IEC 2382-37 Standard on the harmonisation of biometric vocabulary. Scientific definitions mentioned in this section can be found in Table 2.

[42] René McIver, 'Biometric Vocabulary Standardization' in Stan Z Li (ed), *Encyclopedia of Biometrics* (1st edn, Springer 2009) 158.

[43] A working group, Working Group 1, was established within the Subcommittee 37 (Subcommittee on Biometrics) of the Joint Committee 1 of the ISO/IEC, in charge of standardisation in the field of biometrics. For further details, see <www.iso.org> accessed 20 July 2015.

### *a. Several Scientific Disciplines, Several Meanings*

From an etymological point of view,[44] the term 'biometrics' refers to the words 'bio' and 'metrics', both deriving from ancient Greek. 'Bio' finds its origin in the Greek word βίος ('bios'), which means *life*. 'Metric' derives from the Greek words 'metrikos' or 'metron', which means *measurement.* From the etymology of the term, one could infer that 'biometrics' is the science that measures life attributes.[45] However, this definition is too simplistic and does not reflect the multifaceted nature of the term.

Glossaries of biometric terms, such as the 1999 Glossary of Biometric Terms of the Association for Biometrics (AfB) and of the International Computer Security Association (ICSA) or the Biometric Glossary of the US NSTC, show the diversity of situations in which the term might apply. In the 1999 Glossary of Biometric Terms, 'biometrics' is defined in its singular form as a measurable biometric characteristic, whereas in the Glossary of the NSTC, biometrics means both biometric characteristic[46] and biometric process.[47]

In another report written by a committee under the US National Research Council (the Whither Biometrics Committee),[48] the notion of 'biometrics' is deemed to cover two different fields. The first one has emerged at the beginning of the 20th Century as the application of statistics to the field of biology. In that context, biometrics is a synonym of 'biometry'.[49] The discipline has then evolved into biostatistics to cover the application of statistical and mathematical methods to many other fields. These include among others medicine, agriculture, biology, biophysics, and genetics.[50] More recently, with the growing use of automated systems to identify individuals, a second meaning has appeared. Biometrics is defined in that context as 'the automated recognition of individuals based on biological and behavioural traits'.[51] According to the Whither Biometrics Committee, this second field dates back to the 1980s.[52] In the context of this article, the second meaning only is of interest.

In 2002, the Joint Committee (JTC1) of the ISO/IEC established a new Subcommittee, SC 37, on Biometrics. The goal of the Subcommittee is to develop standards for biometrics. Among the six working groups created to support the tasks of the Subcommittee, Working

[44] See, for example, V Zorkadis and P Donos, 'On Biometrics-Based Authentication and Identification from a Privacy-Protection Perspective: Deriving Privacy-Enhancing Requirements' (2004) 12 IMCS 125.
Salil Prabhakar, Sharath Pankanti, and Anil Jain, 'Biometric Recognition: Security and Privacy Concerns' (2003) 1(2) IEEE Security & Privacy 33.
[45] ibid.
[46] Biometrics Glossary (2006) (n 11) 4.
[47] ibid.
[48] Composed of members from the industry and academia from different disciplines, the Whither Biometrics Committee was appointed to write a report on biometric recognition.
[49] Francis Galton, 'Biometry' (1901) 1 Biometrika 7.
[50] Chin Long Chiang and Marvin Zelen, 'What is Biostatistics?' (1985) 14 (3) Biometrics 771.
Whither Biometrics Committee, *Biometric Recognition* (n 12) 16-17.
[51] For example, Anil Jain, 'Biometric Authentication' (2008) 3 (6) Scholarpedia 3716.
[52] Whither Biometrics Committee, *Biometric Recognition* (n 12) 16-18.

Group 1 (WG 1) is responsible for harmonising the vocabulary used in the field of biometrics.[53] The International Standard ISO/IEC 2382-37 is the result of its work.

### *b. Towards a Harmonised Definition of the Term 'Biometrics' in ISO/IEC 2382-37*

The International Standard provides a definition of 'biometrics' and clarifies in that context correct and incorrect usages of the term.

The term 'biometric(s)' is mentioned under three different entries: 'biometric' as an adjective,[54] 'biometrics' as a plural noun (defined under 'biometric recognition'),[55] and 'biometric' as a singular noun (defined under 'biometric characteristic').[56] According to the International Standard, 'biometric' should either be used in its adjective or plural forms. But it should not be used as a singular noun.[57]

As an adjective, the term means 'of or having to do with biometrics'.[58] Biometrics, as a plural noun, is described as the 'automated recognition of individuals based on their biological and behavioural characteristics'.[59] According to the Standard, recognition covers the two functions of a biometric system, i.e. the verification of identity and the identification of an individual.[60] The adjective 'automated' refers to a machine based system (…) either for the full process or assisted by a human being'.[61] Finally, the Standard acknowledges the existence of biostatistics since it clarifies that 'the general meaning of biometrics encompasses counting, measuring and statistical analysis of any kind of data in the biological sciences including the relevant medical sciences'.[62]

It should be noted that even if ISO/IEC Standards do not have a binding effect - unless imposed by law at national level - they are likely to be followed by governments and industries.[63] In the case of the International Standard ISO/IEC 2382-37, the Italian Data Protection Authority ('the Garante') has already acknowledged the authority of the Standard in its Guidelines on Biometric Recognition and Graphometric Signature. In that document, the Garante 'considers it necessary to use the definitions to be found in ISO/EC 2382-37 (…) in order to rely on the harmonized wording in a highly technical context'.[64]

---

[53] For further details on the history of ISO/IEC JTC1, see <https://jtc1history.wordpress.com/sc-37-r2013/> accessed 20 July 2015.
[54] ISO/IEC 2382-37, term 37.01.01.
[55] ISO/IEC 2382-37, term 37.01.03.
[56] ISO/IEC 2382-37, term 37.01.02.
[57] ISO/IEC 2382-37, term 37.01.01, the use of 'biometric' as a synonym of 'biometric characteristic' is deprecated. As a wrong use of the term, the Standard gives the following example: 'the biometric recorded in my passport is a facial image.'
[58] ISO/IEC 2382-37, term 37.01.01.
[59] ISO/IEC 2382-37, term 37.01.03.
[60] ISO/IEC 2382-37, term 37.01.03, Note 3.
[61] ISO/IEC 2382-37, term 37.01.03, Note 4.
[62] ISO/IEC 2382-37, term 37.01.03, Note 1.
[63]< www.iso.org> accessed 20 July 2015.
[64] Garante (n 10) 3.

As a consequence, and in accordance with the International Standard ISO/IEC 2387-32, 'biometrics' as a noun should only be used to mean 'automated recognition'. Any other uses, and in particular as a synonym of 'biometric characteristic', should be excluded. The two glossaries mentioned above therefore contain definitions that do not comply with the International Standard.[65]



***Table 2: Definitions of 'Biometrics' by the Scientific Community***

| Scientific sources | Definitions of 'biometrics' |
|---|---|
| **1999 Glossary of Biometric Terms** | (Singular form): A measurable, physical characteristic or personal behavioural trait used to recognise the identity or verify the claim identity of an enrolee |
| **Biometric Glossary** | 1. *Characteristic*: measurable biological or behavioural aspects of the person that can be used for automated recognition<br>2. *Process*: automated methods of recognising an individual based on measurable biological and behavioural characteristics |
| **Report on Biometric Recognition** | 1. Synonym of biometry<br>2. Automated recognition of individuals based on biological and behavioural characteristics |
| **ISO/IEC 2382-37 Standard** | 1. As an adjective: of or having to do with biometrics<br>2. As a noun (plural): automated recognition of individuals based on their biological and behavioural characteristics |

To conclude this section, on the scientific side, the existence of several definitions for the term 'biometrics' reflects not only the existence of different disciplines, but also different understandings about the function of biometric technologies. However, with the adoption of the International Standard ISO/IEC 2382-37, the term should only be used to mean the 'automated recognition of individuals based on their biological and behavioural characteristics'.

On the legal side, the multiple definitions of the term create confusion and fuzziness. It is true that the Article 29 Data Protection Working Party has (almost) always used the term 'biometrics' as a synonym of 'biometric data'. Yet, there are a few exceptions in its

[65] Here it should be noted that the Biometrics Glossary of the US National Science and Technology Council should have been adjusted to the International ISO/IEC Standard as it provided in its introduction that 'the subcommittee (in charge of the Glossary) w(ould) review th(e) Glossary for consistency as standards (ie the ones by ISO/IEC) are passed', and Biometrics Glossary (n 11) 1.

Opinions that create confusion.[66] As for the EDPS, the European body seems to follow the analysis made by the Article 29 Working Party in its own Opinions. But this is partially true as its glossary of terms contains a different definition for the term 'biometrics'. Finally, bodies related to the Council of Europe define 'biometrics' in a way closer to the scientific definition of the term. As a result to avoid any confusion, when the term 'biometrics' is used in a data protection and privacy context, the term should exclusively refer to the definition contained in the International Standard, i.e. it should mean 'automated recognition'. In other cases, the term should not be used. Some authors have even argued that the term 'biometrics' should not be used at all because of the confusion that its historical and traditional meanings can create. Instead, the term should be exclusively replaced by the expression 'biometric recognition'.[67]

After having clarified the meaning of 'biometrics' and the conditions under which the term should be used in a data protection and privacy context, the article investigates the meanings of 'biometric data' for the biometric and European data protection communities.

## III. Biometric Data: A Technical and a Legal Notion

The second section of the article explores how the term 'biometric data' has been defined and conceived from a scientific perspective and a data protection and privacy perspective. It will also assess whether the legal definition of the term should reflect the technical processing of an individual's data and if so, which technical criteria are missing in the legal definition(s) of the term.

Defining the notion of 'biometric data' is essential to determine the regime of data protection and privacy that can apply to this type of (personal) data.

### 1. Notion Defined by the Biometric Community

In the different scientific sources,[68] the term 'biometric data' relates to or is defined as a 'biometric sample' or 'aggregation of biometric samples'. The Biometric Glossary elaborated by the US NSTC provides a broader definition as it considers 'biometric data' as 'a catch-all phrase for computer data created during a biometric process. It encompasses raw sensor observations, biometric samples, models, templates and/or similarity scores (…).'[69] All relevant definitions are recapped in Table 3.

The different scientific definitions (glossaries, encyclopaedia) are linked to the technical transformation of the biometric characteristics into templates. The definition contained in

[66] See Opinion 3/2012 (n 7) and examples provided in footnotes 30 and 31 of this article.
[67] Anil Jain, Arun Ross, and Karthik Nandakumar, *Introduction to Biometrics* (1st edn, Springer, New York, Dordrecht, Heidelberg, London, 2011) 2.
[68] 'Biometric Data', in SZ Li (ed.), *Encyclopedia of Biometrics* (1st edn, Springer, New York, 2009) 81.
ISO/IEC 2383-37, term 37.03.06.
Glossary of Biometric Terms (n 11).
[69] Biometrics Glossary (n 11) 5.

the ISO/IEC 2382-37 refers in particular to the different phases of a biometric system.[70] Biometric data are therein described as 'biometric sample or aggregation of biometric samples at any stage of processing, e.g. biometric reference, biometric probe, biometric feature or biometric property'.

The ISO/IEC Standard therefore considers the following as biometric data: (a) the capture of the data ('biometric sample'),[71] (b) the extraction of the data contained in the sample ('biometric feature'),[72] (c) the attribution of stored biometric samples to a specific individual for comparison use ('biometric reference'),[73] and (d) the comparison ('biometric probe').[74]



The description of 'biometric data' in the International Standard leads to several remarks. First of all, the Standard does not provide much detail on the definition itself except that it expressly specifies that the notion 'needs not to be attributable to a specific individual'.[75] This is precisely this non-criterion that distinguishes the notion of 'biometric data' in a data protection context from the notion in the scientific context. That link between an individual and his or her biometric characteristics is at the heart of the data protection framework. It allows the identification of individuals. The identification, or better said the identifiability,[76] of an individual is fundamental to the notion of 'biometric data' in a personal data context.[77]

Second, as defined in the Standard, the terms 'biometric features' and 'biometric characteristics' are absolutely not synonymous. 'Biometric feature' corresponds to 'numbers or labels extracted from biometric samples and used for comparison'[78] and is thus limited to the information extracted from the biometric sample. 'Biometric characteristic' exists independently of the technical process of information extraction. The term is defined as 'biological and behavioural characteristics of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition'.[79] Examples of biometric characteristics are finger topography, finger ridge patterns, and retinal patterns.[80]

[70] These phases are usually the enrolment, storage, acquisition, and matching of the data.
[71] ISO/IEC 2382-37, term 37.03.21; defined as "analog or digital representation of biometric characteristics prior to biometric feature 'extraction'."
[72] ISO/IEC 2382-37, term 37.03.11; defined as 'numbers or labels extracted from biometric samples and used for comparison.'
[73] ISO/IEC 2382-37, term 37.03.16; defined as 'one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison.'
[74] ISO/IEC 2382-37, term 37.03.14; defined as 'biometric sample of biometric feature set input to an algorithm for use as the subject of biometric comparison to a biometric reference.'
[75] ISO/IEC 2382-37, term 37.03.06.
[76] The identifiability is the ability to identify an individual from his or her data.
[77] Opinion 4/2007 (n 33).
[78] ISO/IEC 2382-37, term 37.03.11.
[79] ISO/IEC 2382-37, term 37.01.02.
[80] ISO/IEC 2382-37, examples under term 37.01.02.

***Table 3: Notion of 'Biometric Data' as defined by the Biometric Community***

| Scientific sources | Definitions of 'biometric data' |
|---|---|
| **1999 Glossary of Biometric Terms** | Information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data). |
| **The Biometric Glossary** | A catchall phrase for computer data created during a biometric process. It encompasses raw sensor observations, biometric samples, models, templates and/or similarity scores. Biometric data is used to describe the information collected during an enrolment, verification, or identification process, but does not apply to end user information such as user name, demographic information and authorizations. |
| **Encyclopedia of Biometrics** | Any data record containing a biometric sample of any modality (or multiple modalities), whether that data has been processed or not. Biometric data may be formatted (encoded) in accordance with a standard or may be vendor specific (proprietary) and may or may not be encapsulated with the metadata. |
| **ISO/IEC 2382-37 Standard** | Biometric sample or aggregation of biometric sample at any stage of processing, e.g. biometric reference, biometric probe, biometric feature or biometric property. |

### 2. Notion Defined by the Legal Community in the Data Protection and Privacy Context

Not surprisingly Convention 108 and the Data Protection Directive do not mention the term 'biometric data'. At the time of their respective adoption (1980 and 1995), the topic of 'biometric data' and the application of data protection rules to biometric technologies were not widely discussed. One of the first documents to address biometric issues is the *working document on biometrics* released in 2003 by the Article 29 Data Protection Working Party.[81] But it is not until 2007 that the Working Party defines the term 'biometric data' in its generic Opinion on the concept of personal data, Opinion 4/2007.[82] That definition has been referred by the EDPS, in particular in its Opinion on the Turbine project.[83] In 2012, the European Commission proposed to add a definition of 'biometric

[81] A29WP, Working document on biometrics (n 26).
[82] A29WP, Opinion 4/2007 (n 33).
[83] A29WP, Opinion on the Turbine Project (n 35).

data' in the future regulatory framework of data protection.[84] Both the EP and the Council of the EU have amended the proposed definition during their respective vote and political agreement on the proposal of the GDPR.[85] In parallel, at the level of the Council of Europe, the Consultative Committee of Convention 108 has taken a different stance. In the latest draft explanatory report of the modernisation of Convention 108, the Consultative Committee has defined the term by reference to the technical process of extraction of biometric information.[86]



The exact wording of the different definitions proposed by the European bodies and institutions can be found in Table 4. Instead of presenting each of them in a chronological or linear order, common criteria have been extracted and their relevance assessed. The following three criteria are discussed below: (1) the qualification of 'biometric data' as personal data, (2) their link to biometric characteristics, and (3) their characteristic of 'uniqueness'. In addition, at the end of the section, the article explores whether one or several criteria, extracted from the technical definition of the term, should be added to the legal definition of the term.

***a. Qualification as Personal Data***

Among the different legal definitions reviewed, only the one amended by the EP and the Council of the EU explicitly link biometric data to the notion of 'personal data'. In the original proposals of the Data Protection Reform Package, the European Commission has broadly defined 'biometric data' as 'any data relating to (biometric) characteristics' (underline added).[87] During the numerous discussions on the many EP's amendments to the European Commission's proposals, the adjective 'personal' was added to the definition for a 'linguistic clarification'.[88] This is the unique justification that can be found in the written reports of the parliamentary amendments. In the impact assessment accompanying both proposals of the Data Protection Reform Package, the European Commission has implicitly recognised 'biometric data' as a category of 'personal data'. It states that one of the possible legislative options to revise the data protection framework could be to add, among others, 'biometric data' to the category of sensitive data.[89] Yet, sensitive data are a specific category of personal data.[90]

[84] Data Protection Reform Package (n 1).
[85] European Parliament, legislative resolutions on the data protection reform package (2014) (n 4), and Council of the EU, political agreement (n 5).
[86] Council of Europe, Consultative Committee, Draft Explanatory Report (2013) (n 18).
[87] See, respectively, original art 4(11) of the proposed General Data Protection Regulation and original art 3(11) of the proposed Directive on law enforcement (n 2 and n 3).
[88] See JP Albrecht (rapporteur), Draft report on 'the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', PE 506.145v01-00, amendment 778 proposed by Alexander Alvaro, 101.
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-506.145+01+DOC+PDF+V0//EN&language=EN > accessed 20 July 2015.
[89] SEC (2012) 72 final (n 36) 52 and 56.
[90] art 8, para 1, Directive 95/46 EC.

Without labelling 'biometric data' of 'personal data', other institutions have, however, acknowledged the nature of 'biometric data'. This is the case of the Article 29 Data Protection Working Party, which has stated that 'biometric data are in most cases personal data'.[91] The EDPS has also reproduced the argument of the Working Party in its own Opinions.[92]

At the level of the Council of Europe, the different bodies involved in biometric issues have made thorough analysis and claimed for a need to clarify the definition and the type of legislation covering these data.[93] Finally, it should be mentioned that the Consultative Committee of Convention 108 has refused to take position on the issue in its Progress Report of 2005, quoting arguments pro and con the qualification of 'biometric data' as 'personal data'.[94] Yet, the Consultative Committee has concluded that 'as soon as biometric data are collected with a view to automatic processing there is the possibility that these data can be related to an identified or identifiable individual'[95] and thus be personal data.

What does it mean to classify biometric data as personal data? To understand it, a cross-reference to the definition of personal data is necessary. In the resolutions adopted by the EP and the political agreement of the Council on the General Data Protection Regulation, personal data is defined as 'any information relating to an identified or identifiable person (…) (underline added); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person'.[96] This definition of personal data is very similar to the definition contained in current Article 2 (a) of the Data Protection Directive.[97] Classifying biometric data among personal data therefore means that biometric data have the ability to identify individuals.

The definition proposed by the European Commission and amended by the EP and the Council does not reflect the position of the Article 29 Data Protection Working Party on the specificities of 'biometric data'. In its Opinion on *the concept of personal data*, the Working Party has characterised 'biometric data' as both 'content of information' about an individual and 'a link between one piece of information and the individual'.[98] The Working Party has also introduced a flimsy distinction between 'biometric data' and the source

[91] See A29WP, Opinion 3/2012 (n 7) 3, making reference to its Working Document on biometrics.
[92] See, for example, A29WP, Opinion on the Turbine project (n 35).
[93] See, for example, Haibach Report (n 17) para 64.
[94] Progress Report (n 16) para 50.
[95] Progress Report (n 16) para 51.
[96] See respectively amended art 4(2) of the proposed General Data Protection Regulation by the European Parliament (n 4) and amended art 4(2) of the proposed General Data Protection Regulation as agreed by the Council in June 2015 (n 5).
[97] Current art 2(a) Directive 95/46/EC reads as follows: " 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."
[98] A29WP, Opinion 4/2007 (n 33) 8.

from which they are extracted. According to the Working Party, the sources themselves – such as human tissues – should not be considered as 'biometric data' and should not be subject to data protection rules.[99] As observed by some authors, this distinction is, however, very questionable since it does not take into account progress of biometric technologies that might allow in the future the direct extraction of identifying elements from the human tissues themselves.[100] But as said, neither the European Commission nor the European Parliament has followed this position.


Regarding the format under which biometric data are available (i.e. raw data, captured image, or biometric template), none of the definitions under review makes a reference to it. In its Opinion 4/2007 *on the concept of personal data*, the Article 29 Data Protection Working Party has considered that any format on which personal data are stored or contained is relevant.[101] Concerning more specifically biometric data, the Working Party seems to have introduced in its *working document on biometrics* a distinction between biometric information in a raw form and biometric information captured on a template. While raw biometric information would qualify as personal data, information contained in a biometric template would be considered as personal data unless 'no reasonable means c(ould) be used to identify the data subject'.[102] The Working Party has added the condition in a footnote without providing further explanation on its meaning or on the criterion of 'reasonable means.'[103]

In the end, whether or not biometric templates are personal data is not very relevant to the definition of biometric data. It is more relevant for the assessment of the legal regime of protection applicable to them. But this issue is not covered in the current article. In addition, the definition of biometric data should not contain any reference to the existing formats. First of all, referring to specific formats in the definition will limit the application of the data protection rules to these formats. Second, no one can forecast the state of science in a couple of years. Formats that are currently unknown will be used in the future.

#### *b. From Biometric Characteristics to 'Data relating to' Biometric Characteristics*

Through the different reports, opinions, and legislative proposals, the term 'biometric data' has been described as either 'biometric characteristic' or 'data relating to biometric characteristic'.

Definitions of the Article 29 Data Protection Working Party,[104] the EDPS[105] - by reference to the Working Party's works, and the PACE[106] are all focused on biometric characteristics.

[99] A29WP, Opinion 4/2007 (n 33) 9.
[100] For further reading, see criticism in Kindt (n 15) 107, fn 71.
[101] A29WP, Opinion 4/2007 (n 33) 7.
[102] A29WP, Working Document on Biometrics (n 26), see fn 11 of the document.
[103] For further reading, see analysis made in Kindt (n 15) 111-114.
[104] A29WP, Opinion 4/2007 (n 33) 8.
[105] See, for example, A29WP, Opinion on Turbine (n 35).

Examples of these data are constituted by 'fingerprints, retinal patterns, facial structure, voices, but also hand geometry, vein patterns or even some deeply ingrained skills or other behavioural characteristic (such as handwritten signature, keystrokes, particular way to walk or to speak)'.[107] These 'typical' examples provided by the Working Party contrast with the list of examples provided in the Haibach report. The report contains examples of representations (such as images, pictures, or recording) of biometric characteristics and not examples of biometric characteristics themselves.[108] One could argue that biometric data, as understood and illustrated in the Haibach report, are 'data' about biometric characteristics and not biometric characteristics themselves.

The European Commission, the EP and the Council in their respective vote and agreement on the GDPR, and the Council of Europe have all understood 'biometric data' as '[personal] data relating to' biometric characteristics. The use of the preposition 'relating to' raises some issues as to the scope of the definitions: Do biometric characteristics also fall within scope of the definition? Or should only data about biometric characteristics (such as images, recording, or algorithms of biometric characteristics) fall within that scope? The answer to the questions is not easy as none of the preparatory documents of the European Commission, the EP, or the Consultative Committee in charge of revising Convention 108 provides clarity on these issues.[109] The only hint that the European Commission provides is contained in the definition of 'biometric data'. In the proposals of the Data Protection Reform Package, the European Commission illustrates the definition of 'biometric data' with the examples of 'facial images and dactyloscopic data'.[110] Dactyloscopic data have been elsewhere defined as 'fingerprint images, images of fingerprint latents, palm prints, palm print latents and templates of such images'.[111] The examples only relate to representations of biometric characteristics. As a consequence, only those representations and not the biometric characteristics themselves would logically fall within the scope of biometric data and thus personal data. In the end, it is not the fingerprint itself– defined as 'the unique patterns that exist on the underside of every human finger'- but the image of that fingerprint (also called 'fingerprinting' or 'finger scanning')[112] that matters from a personal data perspective.

[106] Haibach Report (n 17).
[107] A29WP, Opinion 4/2007 (n 33) 8.
[108] Haibach Report (n 17) 6, para 5: 'fingerprint images, pictures of the iris or the retina, but also voice recording, individual gait or typing rhythm during logon'.
[109] See, for example, SEC (2012) 72 final (n 36).
Council of Europe, Consultative Committee, Draft explanatory report (2013) (n 18).
[110] Respectively art 4(11) of the proposed General Data Protection Regulation and art 3 (11) of the proposed Directive on law enforcement (n 2 and n 3).
[111] Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L 210/12, see art 2 (i).
[112] See Yue Liu (n 14) 39.

### *c. Uniqueness*

The legal definitions under review refer to the 'uniqueness' of biometric characteristics. Before explaining its meaning from a scientific point of view, one should note that the different European bodies and institutions have merely stated that biometric characteristics are unique or that they can be used for 'unique identification'. But none of them has explained or demonstrated it. They have all referred to it as an established fact.

In the biometric literature, it is commonly accepted and asserted that biometric characteristics are unique.[113] And because they are unique, they can be used for human recognition, i.e. to authenticate individuals or identify them. However, many forensic scholars have criticized this assumption.[114] According to them, it has never been demonstrated, for example, that fingerprints are unique. This assumption might even be 'unprovable'.[115] Nancy Yue Lui, a legal scholar, takes a different stance in the debate. According to her, if the assumption following which biometric characteristics are 'unique' has never been proven, 'there is not yet any solid proof that this assumption is incorrect either'.[116] She, therefore, considers that the 'uniqueness' of biometric data is relative. Forensic scholars on their side believe that the issue for identification is not so much whether biometric characteristics are unique but whether they originate from the same source.

In the Data Protection Reform Package as well in the latest version of the draft explanatory report of revision of Convention 108, the emphasis is not put on the uniqueness of biometric characteristics but on their function. Biometric characteristics are therein defined as 'allow[ing] the unique identification of [an individual]'.[117] Previously mentioned in the works of the Article 29 Data Protection Working Party,[118] this function has not been further explained. It has been considered by some that biometric data, due to their uniqueness, could be used as 'unique identifiers' and could link all information about an individual.[119] The author of the article considers the expression 'unique identification' unfortunate. It might convey the wrong impression about the functions of biometric data by reducing their role to the identification of individuals (i.e. the establishment of their

[113] See among others, Li (n13).
[114] For example, Mark Page, Jane Taylor and Matt Blenkin, 'Uniqueness in the Forensic Identification Sciences: Fact of fiction?' (2011) 206 Forensic Science International 12; David Kaye, 'Questioning a Courtroom Proof of the Uniqueness of Fingerprints' (2003) 71 International Statistical Review 521; Michael Saks, 'Forensic Identification: From a Faith-Based "Science" to a Scientific Science' (2010) 201 Forensic Science International 14.
[115] Simon Cole, 'Is Fingerprint Identification Valid? Rhetorics of Reliability in Fingerprint Proponents?' (2006) 28 (1) Law & Policy 109.
[116] Yue Liu (n14) 67.
[117] See art 4(11) of the proposed General Data Protection Regulation and art 3(11) of the proposed Directive on law enforcement (n 2 and n 3).
Council of Europe, Consultative Committee, Draft explanatory report (2013) (n 16) para 56, 13.
[118] A29WP, Working document on biometrics (n 26), and A29WP, Opinion 4/2007 (n 33).
[119] A29WP, Working document on biometrics (n 26).
Data Protection and Privacy Commissioners, 'Resolution on the Use of Biometrics in Passports, Identity Cards and Travel Documents', 27th Conference, Montreux, 16 September 2005.
<http://www.cnpd.pt/bin/actividade/Outros/biometrie_resolution_e.pdf > accessed 20 July 2015.

identity). Besides identification, biometric data are also largely used to authenticate individuals (i.e. verify their identity).[120]

As a consequence, and because the 'uniqueness' of biometric characteristics is not established, the legal definition of 'biometric data' should not refer to this criterion. In addition, if the assumption were true, why would the legal definition only refer to that criterion? There are at least seven other criteria used to assess whether biometric characteristics are fit for human recognition.[121] 'Uniqueness' is only one of them.

From the analysis of the three common criteria, it can be concluded the importance of identifying biometric data as personal data and limiting the scope of their definition to the 'data relating' to biometric characteristics. For the reasons explained above, the third criterion relating to the questionable 'uniqueness' of biometric characteristics should not be part of the definition. After having assessed the criteria contained in the different legal definitions, the question becomes whether criteria extracted from the scientific definition should be used in the legal definition.

#### *d. Link to the Biometric Processing of the Data, Missing Criterion?*

As shown in Table 4, most of the proposed regulatory definitions for the term 'biometric data' do not mention the technical process of extraction of biometric information and its transformation into a digital template. Only the definitions proposed by the Consultative Committee of Convention 108 and by the Council of EU in its political agreement refer to the 'specific technical processing' of biometric data. However, none of them refers to the automatic process that allows the identification of individuals or the verification of their identity.

Some authors consider that the proposed legal definitions fail to take into account, in particular, the use of 'automated means' to process biometric data and the purposes of biometric characteristics. Based on these two missing elements, Els Kindt has proposed the following new legal definition to the term 'biometric data': 'all personal data which (a) relate directly or indirectly to unique or distinctive biological or behavioural characteristics of human beings and (b) are used or fit to be used by automated means (c) for purposes of identification, identity verification or verification of a claim of a living natural person'.[122]

Her definition calls for several comments. First of all, should the definition of biometric data specify that biometric data are processed by automated means? This seems at least not necessary in the context of the revision of Convention 108 as the Convention only

[120] James L Wayman, 'Biometric Verification/Identification/Authentication/Recognition: The Terminology' in Stan Z Li (ed.), *Encyclopedia of Biometrics* (1st edn, Springer 2009), 153-157.
[121] Jain, Ross and Nandakumar (n 67), see universality, uniqueness, permanence, measurability, performance, acceptability and circumvention, 29-30.
[122] Kindt (n 15) 149.

applies to automatic processing of personal data.[123] This precision is, however, debatable in the context of the current Data Protection Directive as the text applies to both automatic processing and paper-based processing of data.[124] The advantage of referring to 'automated means' is to avoid ambiguity while allowing future technological developments. The term is indeed technologically neutral.[125] Second, should the purpose(s) of biometric characteristics be spelled out in the legal definition of biometric data? The way Els Kindt describes the purposes of biometric characteristics is more accurate than in the proposals of definitions contained in the Data Protection Reform Package and in the Draft explanatory report of revision of Convention 108. The proposed definitions are limited to the purpose of 'identification'. But should the definition be specific about the purposes and describe them? By doing so, there is a risk that future way of recognising individuals might not be taken into account. Instead, the regulatory definition(s) should refer to the generic term of 'recognition', which is meant to cover both identification and verification of individuals.[126] Adding the purposes of biometric data would accurately reflect their current uses by the different communities (i.e. scientific, law enforcement or forensic ones).

Finally, it is legitimate to question whether the formats of biometric data (raw data, sample, template) should be added to the definition. By doing so, there is a risk to limit biometric data to the currently existing formats. As any reference to the formats should instead remain technology neutral, the regulatory definitions should at the best refer to the expression 'biometric data, whatever their form'.

The definition of 'biometric data' proposed by the European Commission and amended by the EP and the Council of the EU does not refer to the technical process of extraction of information and its transformation into a biometric template. Neither does it refer to the automatic processing that allows the identification or the verification of identity. These technical aspects are completely absent from the proposed legal definition. However, for the reasons explained above, the legal definition of 'biometric data' should remain technologically neutral and not mention any format or the technical processing of data. Finally, it should be noted that in the absence of adoption of the Data Protection Reform Package,[127] the legal definition that prevails for the time being at the EU level is the one provided by the Article 29 Working Party. At the level of the Council of Europe, no definition prevails in the absence of authoritative sources.

[123] art 3, scope, Convention 108.
[124] art 3, scope, Directive 95/46/EC.
[125] Jeroen Terstegge, 'Article 3 Directive 95/46/EC' in Alfred Büllesbach, Serge Gijrath, Yves Poullet and Corien Prins (eds), *Concise of European IT law* (2nd edn, Kluwer Law International 2010), 42-43.
[126] ISO/IEC 2382-37, term 37.01.03, entry 'biometric recognition', Note 3.
[127] The negotiations are currently at the level of the Council.

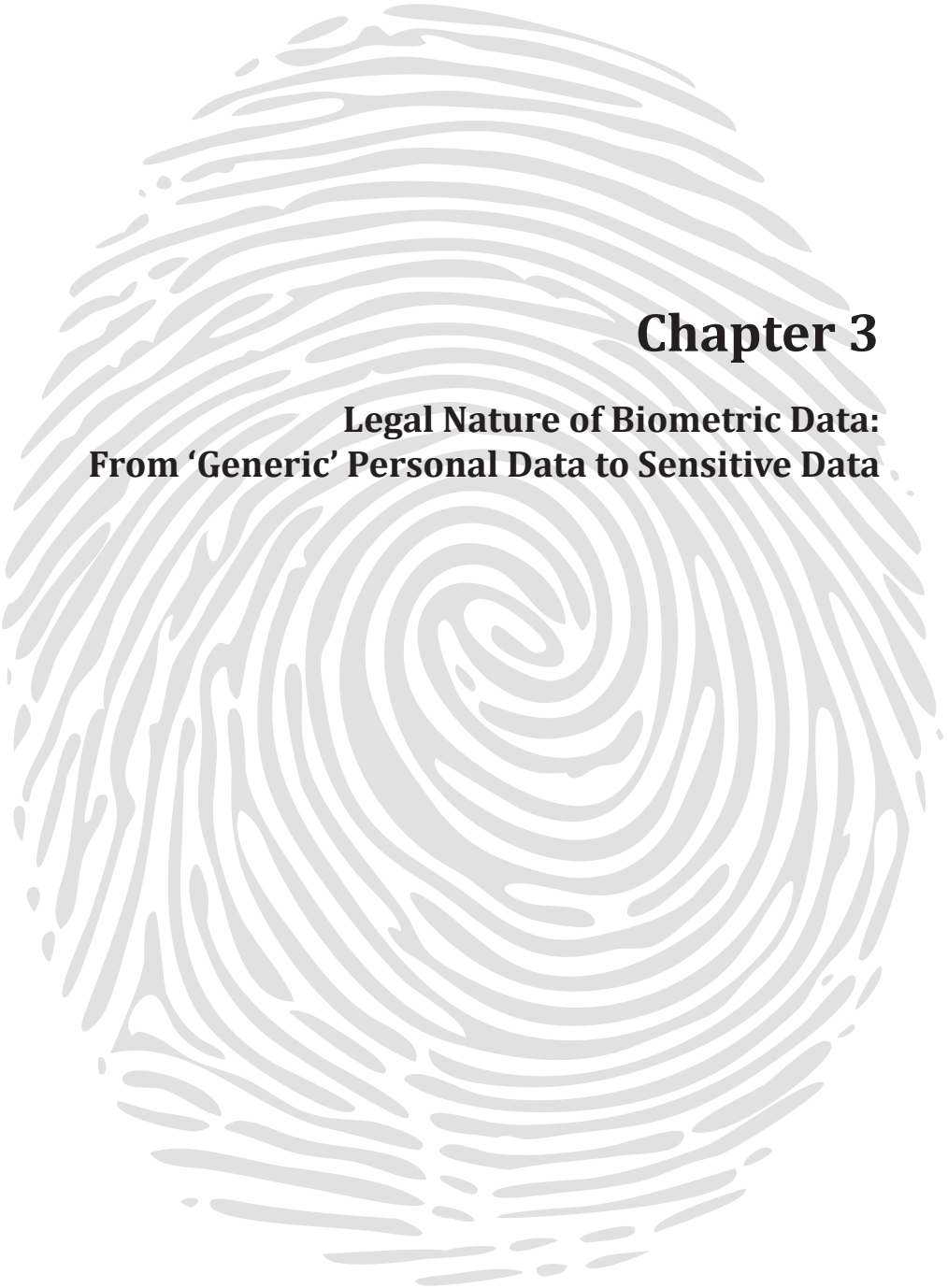
***Table 4: Notion of 'Biometric Data' as defined by the Legal Community in the Data Protection and Privacy Context***

| European bodies/institutions | Definitions of 'biometric data' |
|---|---|
| **Article 29 Working Party and EDPS** | Biological properties, physiological characteristics, living traits, or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability.<br>(Opinion 4/2007), Definition quoted by the EDPS in Opinion on the Turbine project (2011) |
| **PACE** | Unique physical or behavioural characteristics that differ from one human being to another and that remain, in most cases, unaltered for life.<br>(Haibach report, 2011) |
| **Consultative Committee of Convention 108** | Data resulting from a specific technical processing of data concerning the physical, biological, or physiological characteristics of an individual which allows the unique identification of the latter.<br>(Draft explanatory report of the modernised version of Convention 108, 10 July 2013) |
| **European Commission and EP** | *Any personal* data relating to the physical, physiological, or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data.<br>(Text added by the European Parliament indicated in italic.)(Article 4(11) of the proposed General Data Protection Regulation and Article 3(11) of the proposed Directive on data protection and law enforcement, 2012)(Resolutions of 12 March 2014 on two proposals of the European Commission) |
| **European Commission and Council of the EU** | *Any personal* data *resulting from specific technical processing* relating to the physical, physiological, or behavioural characteristics of an individual which *allows or confirms the* unique identification of *that* individual, such as facial images, or dactyloscopic data.<br>(Text added by the Council indicated in italic)(Article 4(11) of the proposed General Data Protection Regulation)(Political Agreement of 15 June 2015 on the General Data Protection Regulation) |

## IV. Conclusions

This article has approached two notions regularly used in the European data protection field when addressing issues linked to biometric technologies: the terms 'biometrics' and 'biometric data'. Although often used as synonyms by several European bodies and institutions, the two terms have different meanings. To clarify their respective meanings, this article has explored their definitions from a data protection perspective and compared them with the definitions provided by the biometric community. From this comparison and analysis, it results that most of the European bodies and institutions use the term 'biometrics' in a very confusing way: as a synonym of 'biometric data' but also as a synonym of biometric technologies. However, it appears that the term 'biometrics' has mainly a technical meaning. As a consequence, when used in a data protection context, the term should refer to its technical meaning as set by the biometric community. The text of reference is the current version of the International Standard ISO/IEC 2382-37. In that document, 'biometrics' refers to the automatic recognition of individuals.

The second term, 'biometric data' is more complex as it covers two different realities. From the perspective of the biometric community, it covers the technical process through which the biometric information is captured and transformed into a digital format. From the perspective of the data protection and privacy community, the term is approached as a type of personal data relating to biometric characteristics and linked to the identification or identifiability of an individual. The link to an individual is where the scientific and the legal definitions differ. Fundamental in a data protection and privacy context, that link becomes meaningless in the context of the International Standard. However, the legal definition proposed by the European institutions for the term 'biometric data' appears to be incomplete: it does not take into account the technical processing of biometric data. But should not the legal and the technical definitions remain distinct as they relate to two different contexts? If not, to which extent should the scientific definition be reflected in the legal definition? Although the article has not explored the question, it would be logical to also wonder whether the legal definition should be reflected in the scientific definition. This would open up another way of approaching the notion of 'biometric data' and possibly the relationship between the biometric field and the European data protection field.



# Chapter 3

## Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data

## *Chapter 3: Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data*

*Which Changes Does the New Data Protection Framework Introduce?*[*]

**Abstract:**
*For many years, the status of biometric data from a European data protection perspective generated a lot of discussions among European bodies and legal experts. Finally, after four years of lengthy negotiations, the European institutions have adopted a new data protection framework. For the first time, the concept of biometric data is introduced in a European legislative text. Beyond being defined, biometric data are also treated as sensitive data. The changes introduced by the new data protection framework and the issues they raise will be assessed in this article. In a first section, the article will introduce the topic and clarify some terminological aspects. In a second section, it will summarise the slow introduction of the notion of 'biometric data' into the European data protection landscape before the adoption of the Data Protection Reform Package. The next section will deconstruct the concept of biometric data with the help of the definition of personal data. It will then argue that the threshold of identification required for biometric data is higher than the one required for 'generic' personal data. In a fourth section, the article will assess the 'sensitive data' regime that is applicable to biometric data. It will also question the element of the context of the processing, which has been added as the condition that triggers the extra protection granted to sensitive data. The last section will conclude on the changes introduced by the new provisions.*

### I. Introduction

Payment processing companies, such as MasterCard, are working on developing technologies that use facial images and fingerprints to replace passwords in payment transactions.[1] Other payment companies seem to be working on yet more futuristic passwords, based on edible and embeddable biometric technologies. In April 2015, one of

[*] Article published in the European Data Protection Law review (EDPL), volume 2, issue 3, September 2016, pages 297-311; the author wishes to thank Prof Jeanne Mifsud Bonnici and Prof Laurence Gormley for their comments in an earlier draft, the peer reviewers for their very valuable reviews which helped improve the quality of the article and Christina Angelopoulos for her careful reading and editing suggestions. The views expressed in this article are solely those of the author. All remaining errors are the author's sole responsibility. This research was partly carried out under the European Union's Seventh Framework Programme for research, technological development and demonstration in the context of the INGRESS project (www.ingress-project.eu) under grant agreement no 312792.
[1] Alanna Petroff, 'MasterCard launching selfie payments' *CNN* (22 February 2016) <http://money.cnn.com/2016/02/22/technology/mastercard-selfie-pay-fingerprint-payments/> accessed 30 May 2016.

the executives of PayPal explained that such technologies were under development.[2] In an interview to the Wall Street Journal, he mentioned a shift in identification methods from the 'external body methods like fingerprints, towards internal body functions like heartbeat and vein recognition, where embedded and ingestible devices will allow 'natural body identification'.[3] While the company at stake denied developing such technologies and dissociated itself from the position of its employee, this example nevertheless illustrates the growing and widespread use of biometric data by private parties. Against this background and trends, the establishment of a legal definition and status of biometric data in the new EU data protection framework is welcome.

The concept of biometric data is absent from the European founding texts in the field of personal data protection, i.e. Convention 108[4] and the Data Protection Directive.[5] At the time of their respective adoption, the impact of biometric technologies on data protection rules was not widely discussed. The issue became a hot topic in the early 2000s. In 2003, the Article 29 Data Protection Working Party (the A29WP)[6] issued a *Working Document on biometrics,* in which it addressed the application of data protection rules to biometric systems.[7] Later on, it pursued its analysis in Opinion 3/3012 *on developments in biometric technologies*.[8] In parallel, the European Data Protection Supervisor (the EDPS)[9] discussed the legal status of biometric data from a data protection perspective in the context of the Passport Regulation (Council Regulation 2252/2004)[10] and also of border control instruments (in relation to the establishment of large-scale biometric databases, such as EURODAC, VIS or SIS).[11]



[2] Jonathan LeBlanc, 'Kill All Passwords' (2015)<http://www.slideshare.net/jcleblanc/kill-all-passwords> accessed 30 May 2016.
[3] Amir Mizroch, 'PayPal wants you to inject your username and eat your password' *The Wall Street Journal* (17 April 2015) <http://money.cnn.com/2016/02/22/technology/mastercard-selfie-pay-fingerprint-payments/> accessed 30 May 2016.
[4] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS, No. 108, 28 January 1981, Strasbourg (Convention 108).
[5] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281/23 (Directive 95/46/EC or Data Protection Directive).
[6] The Article 29 Data Protection Working Party is an independent advisory body to the European Commission on data protection matters, composed of representatives of national data protection authorities, of the European institutions, and of the European Commission <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm> accessed 30 May 2016.
[7] A29WP, 'Working Document on Biometrics' [2003] WP80.
[8] A29WP, 'Opinion 3/2012 on Developments in Biometric Technologies' [2012] WP193.
[9] Independent supervisory authority, which monitors the processing of personal data by the EU institutions and bodies, and advises on policies and legislative instruments that impact data protection <https://secure.edps.europa.eu/EDPSWEB/edps/cache/offonce/EDPS/Membersmission > accessed 30 May 2016.
[10] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L385 (Passport Regulation or Regulation No.2252/2004); see EDPS, 'Opinion on the proposal to amend Council Regulation No 2252/2004' [2008] OJ C200/1.
[11] EURODAC is the EUROpean DACtyloscopic database, established in 2000 for the comparison of the fingerprints of asylum seekers; the Visa Information System allows the Member States of the Schengen area to exchange visa data (such as fingerprints) since 2004 and the Schengen Information System (SIS) was set up to support the exchange of information.

The entry into force of the Lisbon Treaty, in 2009, abolished the pillar structure[12] and changed the way data protection is approached at EU level. Prior to that Treaty, due to the pillar structure, a patchwork of instruments regulated the processing of personal data in different sectors. The main instrument on data protection for internal market activities, falling under the 'first pillar', was the Data Protection Directive (Directive 95/46/EC).[13] In 'the third pillar' area of police and judicial cooperation, the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters was the main instrument on data protection.[14] Many sector-based regimes complemented these two instruments.[15] With the entry into force of the Lisbon Treaty, the Charter of Fundamental Rights became binding, granting the status of fundamental right to the right to the protection of personal data, as set in Article 8 of the Charter. In addition, the Treaty of Lisbon introduced a new legal basis, Article 16 of the Treaty on the Functioning of the European Union. That Article gives general competence to the EU institutions to legislate on data protection matters across all sectors. Between 2009 and 2011, the European Commission launched two public consultations on the future of data protection regime.[16] Among the issues discussed was the introduction of the concept of biometric data within the data protection framework. In January 2012, the European Commission proposed a comprehensive data protection framework, the Data Protection Reform Package, regulating all sectors including police and judicial cooperation in criminal matters. The Data Protection Reform Package is composed of a proposal for a General Data Protection Regulation (known as the GDPR and replacing the Data Protection Directive)[17] and a proposal for a Directive on data protection rules applicable to law enforcement activities (replacing the Council Framework Decision 2008/977/JHA).[18] After four years of intensive and lengthy discussions, the new Data

[12] Between 1993 and 2009, the EU was composed of three pillars: the three communities were gathered under the first pillar, Common Foreign & Security Policy under the second pillar, and Police and Judicial Cooperation under the third pillar.

[13] Directive 95/46/EC (n 5).

[14] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L350/60 (Council Framework Decision 2008/977/JHA).

[15] eg Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention [2000] OJ L316/1 (repealed by European Parliament and Council Regulation (EU) No 603/2013 of 26 June 2013); Council Decision of 8 June 2004 establishing the Visa Information System (VIS) [2004] OJ L213/5; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L205/63.

[16] The European Commission launched two public consultations. The first one, in 2009, concerned the future legal framework for the fundamental right to protection of personal data in the European Union. This consultation resulted into a Communication by the European Commission, 'A comprehensive approach on personal data protection in the European Union, published on 4 November 2010 (COM (2010) 609 final)). The European Commission consulted a second time stakeholders on the proposals made in the Communication. <http://ec.europa.eu/justice/newsroom/data-protection/opinion/090501_en.htm> accessed 30 May 2016.

[17] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and of the free movement of such data (General Data Protection Regulation), COM (2012) 11 final [2012] <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN > accessed 30 May 2016.

[18] European Commission, Proposal for a Directive of the European Parliament and of the competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the

Protection framework was officially adopted in April 2016.[19] In both the GDPR and the Directive on law enforcement,[20] the concept of biometric data is defined and added to the list of sensitive data.

This article will address the legal status of biometric data from an EU data protection perspective and assess the impact of the adoption of the Data Protection Reform rules on their status. It will review the provisions contained in the Data Protection Directive and compare them with those of the GDPR. The provisions of the Data Protection Directive will remain applicable until the entry into force of the Data Protection Reform Package.[21] The article primarily focuses on the provisions of the GDPR. However, references to the new data protection framework as a whole might also be made. References to Convention 108 and its draft revision will also be made as a point of comparison, in particular in relation to the qualification of biometric data as sensitive data.[22]


The article builds on existing legal literature pertaining to the status and qualification of biometric data from a data protection perspective. It will analyse, among others, the contributions by Prins, Grijpink, Yue Liu and Kindt.[23] Since the topic is highly technical, references to the scientific literature and terminology used in the biometric field will be made. In particular, the definitions adopted in the International Standard ISO/IEC 2382-37: 2012 on a Harmonized Biometric Vocabulary will be mentioned.[24] It should be noted that, even though the process of standardization is not complete yet, the International Standard can nevertheless be used as a reference. It has already been quoted, in particular, by the Italian Data Protection Authority (Il Garante) in its Guidelines on Biometric

execution of criminal penalties, and the free movement of such data, COM (2012) 10 final; the new Directive does not have any official acronym and is referred to as 'the Directive on law enforcement' in this article.

[19] Adoption of the General Data Protection Regulation and of the Directive on law enforcement on 14 April 2016 <http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776/Data-protection-reform-Parliament-approves-new-rules-fit-for-the-digital-era> accessed 30 May 2016.

[20] European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and of the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1; European Parliament and Council Directive (EU) 2016/680 of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89 (Directive 2016/680).

[21] The Regulation will apply from 25 May 2018 while Member States should have transposed into national law the provisions of the Directive by 6 May 2018; see Art 99 GDPR and Art 63 Directive 2016/680.

[22] Convention 108 (n 4); Draft Explanatory Report to the modernised version of Convention 108, working document of 2 June 2016 <http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Draft%20Explanatory%20report_En.pdf > accessed 30 May 2016.

[23] See Corien Prins, 'Biometric Technology Law, Making Our Body Identify for us: Legal Implications of Biometric Technologies' (1998) 14(3) Computer Law and Security Report 159, 163; Jan Grijpink, 'Privacy Law: Biometrics and Privacy' (2001) 17(3) Computer Law & Security Review 154, 156-157; Yue Liu, 'Identifying Legal Concerns in the Biometric Context' (2008) 3(1) Journal of International Commercial Law and Technology 45; Els Kindt, *Privacy and Data Protection Issues of Biometric Applications, A Comparative Legal Analysis* (Springer 2013).

[24] ISO/IEC 2382-37: 2012 (E)—Information Technology—Vocabulary—Part 37: Biometrics <http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55194> accessed 30 May 2016.

Recognition and Graphometric Signature.[25] Biometric characteristics from which biometric data are extracted are physical or behavioural attributes. These attributes (such as face, fingerprints, voice or gait) show some distinctive and repeatable features (i.e. patterns) that can be measured and compared so as to recognise an individual. Biometric recognition is the general term used to cover the functions of a biometric system based on biometric data. These functions can be split between 'biometric identification', where the identity of an unknown individual is (or is not) established, and 'identity verification', where that individual's identity does not need to be established, but only verified. To perform biometric recognition, biometric characteristics are transformed into data under different formats: a sample (such as the image of a fingerprint, a facial image) and a template (a reduced form of the sample translated into codes, numbers).[26] The technical terms are further explained in the body of the article.

Although this article relies on scientific literature and terminology, it is not written by a scientific expert and it will not assess the quality of the scientific papers to which it refers. The article uses them as descriptive elements.

The article is structured as follows. The next section, Section II, describes the slow introduction of the notion of biometric data in the data protection field at the European level before the adoption of the Data Protection Reform Package. Section III deconstructs the concept of biometric data as defined in the GDPR. To this end, the section describes each component of the definition and assesses in particular the role played by the function of identification. On this issue, the article distinguishes the meaning of identification from a data protection perspective from that from a biometric recognition perspective. Section IV is dedicated to the status of biometric data as sensitive data. It also discusses the relevance of the purpose of processing as a condition for applying the regime of sensitive data to biometric data. The last section concludes on the changes that the GDPR introduces for the legal qualification and status of biometric data from a data protection perspective at EU level, as well as on the remaining uncertainties.

## II. The Slow Introduction of the Notion of Biometric Data in the EU Data Protection Field

This section retraces the progressive recognition of biometric data as a category of personal data at EU level prior to the adoption of the Data Protection Reform Package.[27]

[25] See Il Garante (2014), Annex A to the Garante's Order of 12 November 2014, 3 <http://194.242.234.211/documents/10160/0/GUIDELINES+ON+BIOMETRIC+RECOGNITION> accessed 30 May 2016.
[26] For an overview of biometric recognition, see for instance Yi Chen and Jean Christophe Fondeur, 'Biometric Algorithms' in Stan Z Li & Anil K Jain (eds), *Encyclopedia of Biometrics* (Springer 2015) 156-161.
[27] This section is based on the findings of a previous article, see Catherine Jasserand, 'Avoiding Terminological Confusion between the Notions of 'Biometrics' and 'Biometric Data': an Investigation into the Meanings of the

The concept of biometric data cannot be found in Convention 108[28] nor in the Data Protection Directive,[29] the two European founding texts in the field of personal data protection.[30] This is logical, since at the time of their respective adoption, in 1981 and 1995, the impact of biometric technologies on data protection at European level was not widely discussed. It was not until the early 2000s that the European bodies started to discuss the topic.[31] The first documents and reports on the topic show their hesitations as to the exact status and definition of biometric data.

In 2003, the A29WP issued *a working document on biometrics* in which it addressed the application of data protection rules to biometric systems. While discussing the application of the Data Protection Directive to biometric data, it assessed their status from a personal data perspective. Its early findings on the nature of biometric data are unclear. On one side, it acknowledged that biometric data are by nature personal data, since they always relate to an individual who is 'generally identifiable'.[32] But on the other side, it considered that biometric data are not always personal data. It referred, in particular, to biometric templates, which might not constitute personal data if they 'are stored in a way that no reasonable means can be used by the controller or by any other person to identify the data subject.'[33] As observed by Kindt, the A29WP did not provide any clear criteria to distinguish cases where biometric data (in particular under the form of biometric template) are personal data from the cases where they are not. In the subsequent Opinion on *developments in biometric technologies*, Opinion 3/2012, the Working Party did not provide further explanations. It merely repeated that 'in most cases biometric data are personal data' without further analysis on the definition or on the formats of biometric data.[34]



When reviewing the various opinions and reports on data protection and biometric data, what is striking is the absence of a definition for the notion 'biometric data'. A definition of the term emerged quite late in the discussions on biometric data and technologies.[35] In particular, the A29WP investigated the status of biometric data from a data protection perspective even before defining the notion. It was only in 2007 that the Working Party gave a definition to the concept in Opinion 4/2007 on the *concept of personal data*. In that Opinion, biometric data are approached from a scientific perspective and defined as 'biological properties, physiological characteristics, living traits or repeatable actions

Terms from a European data protection and a Scientific Perspective' (2016) 6(1) International Data Privacy Law 63.

[28] Convention 108 (n 4).

[29] Directive 95/46/EC (n 5).

[30] The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (updated in 2013) are also a non-binding source <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 30 May 2016.

[31] In literature, some authors have addressed the issue earlier, eg Prins (n 23).

[32] A29WP, Working document on biometrics (n 7) 10.

[33] ibid fn 11, 5.

[34] A29WP, Opinion 3/2012 (n 8) 7.

[35] For a complete overview of the definitions proposed by the European bodies, see Jasserand (n 27).

where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability.'[36] In that same opinion, the A29WP argued that biometric data have a dual nature: they are both a piece of information about an individual and constitute a (unique) link between that individual and his or her biometric characteristics. This definition was quoted several times by the EDPS[37] and the A29WP itself.[38] However, that definition does not link 'biometric data' to 'personal data'. It is interesting to note that the definition of biometric data originally contained in the proposals for a Data Protection Reform Package also had no link to personal data.[39]

In their opinions and reports, the European bodies have indistinctly used the terms 'biometric data' and 'biometrics'. However, a systematic analysis of the two notions reveals that 'biometric data' is both a technical and a legal notion, whereas 'biometrics' is only a technical notion.[40] In any case, the two are not synonymous. The term 'biometrics' has been borrowed from the biometric recognition field. As such, in a data protection context, it should only be used in the way defined by the biometric community, i.e. as an 'automatic recognition method' based on biometric characteristics.[41] The term 'biometric data', on its side, covers the technical transformation of biometric characteristics into formats that can be used for biometric recognition. The technical definition does not require a link to a specific individual.[42] By contrast, in a data protection context, this link is crucial to determine whether the technical 'biometric data' constitute personal data. The next section deconstructs the legal concept of 'biometric data' introduced in the Data Protection Reform Package.

### III. Deconstruction of the Legal Concept of Biometric Data

Until the adoption of the Data Protection Reform Package, there was no express provision on the concept of biometric data nor specific rules to regulate the processing of biometric data in European data protection instruments. Article 4(14) GDPR now defines 'biometric data' as:

> 'Personal data' resulting from a specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which

[36] A29WP, 'Opinion 4/2007 on the concept of personal data' [2007] WP136, 8.
[37] EDPS, 'Opinion on a Research Project Funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs)' [2011] (hereinafter Opinion on Turbine Project).
[38] A29WP, Opinion 3/2012 (n 8).
[39] European Commission, Proposal for the General Data Protection Regulation (n 17), Art 4(11) that reads as follows: '*data* resulting from…' (emphasis added).
[40] See Jasserand (n 27).
[41] ISO/IEC 2382-37 (n 24), Term 37.01.03.
[42] ISO/IEC 2382-37 (n 24), Note below term 37.03.06 that reads as follows: 'biometric data need not be attributable to a specific individual.'

allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

The concept can be further analysed through its different components.

**1. Personal Data**

'Biometric data' are first of all personal data. This means that, before legally qualifying as 'biometric', this type of data needs to comply with the criteria applicable to the general category of personal data.

The definition of personal data in Article 4(1) GDPR is very similar to the original definition contained in Article 2(a) of the Data Protection Directive.[43] The notion is indeed defined in identical terms, as 'any information relating to an identified or identifiable natural person ('data subject').' The difference between the two lies in the description of what an 'identifiable person' is. Article 4(1) GDPR contains a broader list of possible identifying factors (including genetic identity) and adds examples of identifiers (such as name, identification number, location data and online identifier). The definition does, however, not refer to the notion of a biometric identity or biometric identifier.


The threshold according to which the identification of an individual is determined remains low: the individual does not need to be identified, but only made identifiable. Like in Article 2(a) of the Data Protection Directive, the adjective 'identified' is undefined.[44] As interpreted by the A29WP in Opinion 4/2007, 'identified' should be understood as meaning to be 'singled out' or 'distinguished' from a group of people.[45] Identifying someone in a data protection context therefore does not require establishing his or her identity.

'Identifiable' is different from 'identified', as the former refers to an individual who has not been identified yet, but who can be, through the combination of other information. Recital 26 GDPR reiterates the test of 'identifiability', originally contained in the Data Protection Directive.[46] That test relates to "all the means likely reasonably to be used" to identify an individual. Recital 26 GDPR also sets a list of factors to be taken into account to assess the identifiability of an individual. That list is based on factors suggested by the A29WP in

[43] art 2(a) of the Data Protection Directive (n 5) reads as follows: 'personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one more factors specific to the physical, physiological, mental, economic, cultural or social identity.'

[44] See also analysis made by Waltraut Kotschy, 'Article 2, Directive 95/46/EC' in Alfred Büllesbach, Serge Gijrath, Yves Poullet and Corien Prins (eds), *Concise of European IT law* (2nd edn, Kluwer Law International 2010), 35.

[45] A29WP, Opinion 4/2007 (n 36) 12-13.

[46] Recital 26 of the Data Protection Directive reads as follows: 'Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person (…).'

Opinion 4/2007.[47] Among those factors are those relating to 'available technology at the time of processing and technological development.'[48]

### 2. Resulting from a Specific Technical Processing

Like the Data Protection Directive, the General Data Protection Regulation regulates the processing of personal data.[49] The processing of personal data is defined in Article 4(2) GDPR as follows:

> Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The regulatory definition of biometric data contains a reference to technical processing. It does not specify what should be understood by 'specific technical processing', except to state that the purpose of that processing should be to uniquely identify an individual. In order to understand the technical processing to which biometric characteristics are subjected and their transformation into data, the following paragraphs explain the technical stages of biometric recognition and the biometric templates resulting from them.

#### *a. Technical Steps of Biometric Recognition*

The first stage of the processing is the enrolment of the biometric characteristics in a biometric system. The biometric characteristics are 'captured' under the form of an image, such as a fingerprint image. The format resulting from this phase is called a biometric sample.[50]

In a second stage, the information contained in a sample is extracted, reduced, and transformed into labels or numbers via an algorithm.[51] This phase is called feature extraction.[52] Only the 'the salient discriminatory information that is essential for recognizing the person' will be kept.[53] The extracted features are kept in a biometric

[47] A29WP, Opinion 4/2007 (n 36) 15.
[48] Recital 26 GDPR reads as follows: 'To determine whether a person is identifiable, account should be taken to all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.'
[49] See material scope, art 3(1) of the Data Protection Directive and Art 2(1) GDPR.
[50] ISO/IEC 2382-37 (n 24), Term 37.03.21, Definition of biometric sample as: 'analog or digital representation of biometric characteristics prior to biometric feature extraction.'
[51] This is a very simplified presentation of the formats. For further technical details, see Kindt (n 23) 43-47.
[52] ISO/IEC 2382-37 (n 24), Term 37.03.21.
[53] eg Davide Maltoni, Dario Maio, Anil Jain, and Salil Prabhakar (eds), *Handbook of Fingerprint Recognition* (Springer 2003) 26.

template under the form of a 'mathematical representation of the original [biometric] characteristic.'[54] The reference template is then stored for comparison.[55]

In a third stage, a biometric sample (such as a fingertip) presented at a sensor will be compared with a previously recorded template (such as the template of a fingerprint). In some cases, the comparison will be established with another biometric sample instead of a template. Comparison between samples is however less common.[56]

From these different technical steps and the transformation of biometric characteristics into biometric information, several processing operations, as defined in Article 4(2) GDPR, can be identified:[57] in a first phase (enrolment), data are collected; during the second phase (feature extraction), data are organised, structured, adapted and stored; the final phase of comparison entails specifically the retrieval, consultation, use and disclosure of the data.


***b. Biometric Formats Resulting from the Technical Processing***

Two formats result from the technical processing: the biometric sample and the biometric template. As already described, a sample is the image of a biometric characteristic, whereas a template is a reduced and encoded form of information contained in a sample. Some authors, as well as the A29WP, wrongly use the phrase 'raw (biometric) data' to designate a biometric sample.[58] Raw (biometric) data are, for example, a fingerprint, fingertip, iris, voice, etc. In the absence of any technical processing through which the raw data are obtained, these fall outside the scope of biometric data. The term 'raw data' should only be used as a synonym of biometric characteristics.

Under the regime of the Data Protection Directive, the issue of biometric formats played an important role in the debate on the legal qualification of 'biometric data'. Not much doubt was expressed on the status of biometric samples, which were considered personal data.[59] In contrast, the status of biometric templates has generated more discussion. The position of the legal literature has also changed over time, taking into account the state of the art in biometric recognition. In early discussions on the nature of biometric templates from a data protection perspective, it was believed that biometric templates could not be 'translated back' into the biometric samples from which they originated. This was the

[54] Emma Wollacott, 'Protection when Tech Gets Rather Personal', Biometrics and Identity Management, *Le Raconteur* (30 April 2015) 10 <https://www.raconteur.net/biometrics-2015 > accessed 30 May 2016.
[55] *Encyclopedia of Biometrics* (n 26), 'Biometric Template', 152, and Andy Adler and Stephan Schuckers, 'Biometric Vulnerabilities, Overview' in *Encyclopedia of Biometrics* (n 26) 164.
[56] Kindt (n 23).
[57] Art 4(2) GDPR, the processing of personal data is defined as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such a collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'
[58] See criticisms by Kindt in Kindt (n 23), fn 100, 43 and fn 39, 98.
[59] Liu (n 23) 45-54; Paul De Hert, 'Biometrics: Legal Issues and Implications', Background Paper for the Institute of Prospective Technological Studies, DG JRC- Sevilla European Commission (2005) 13.

position defended by Prins and Grijpink.[60] Grijpink even argued that biometric templates were anonymous data. Since Prins' and Grijpink's papers were first published, the scientists Adler,[61] Bromba,[62] Ross, Shah,[63] Cain and Jain[64] have demonstrated that biometric templates are in fact partially reversible and could possibly regenerate information contained in biometric samples. In recent legal studies on the legal status of biometric data, authors have concluded that biometric templates are reversible, at least partially, and may not be considered as anonymous data anymore.[65]

The new data protection framework does not refer to biometric formats. This is logical, since the legislative instruments are technology-neutral and the legal definitions should not be tied to any specific format. In any case, the notion of 'information' contained in the definition of personal data and as interpreted by the A29WP,[66] covers any type of form and format.[67] As a result, if discussions on the formats do not have their place in the Data Protection Reform Package, the European Data Protection Board[68] could provide guidance to stakeholders and national data protection authorities on the legal qualification of biometric formats.

### 3. Relating to the Physical, Physiological or Behavioural Characteristics of a Natural Person

This criterion relates to the definition of biometric characteristics. It acknowledges the broad spectrum of measurable human characteristics that can be used for biometric recognition: this covers physical and physiological attributes (such as a fingerprint, face or iris), as well as behavioural attributes (such as voice, gait or signature).[69] The difference between physiological and physical characteristics is not very clear. Many experts in biometric recognition only refer to two types of characteristics: either physical and behavioural characteristics, or physiological and behavioural characteristics.[70] They

[60] Respectively Prins (n 23) and Grijpink (n 23).
[61] Andy Adler, 'Can Sample Images be Regenerated from Biometric Templates?' (Biometrics Conference, 22 - 23 September 2003) <http://www.sce.carleton.ca/faculty/adler/publications/2003/adler-2003-biometrics-conf-regenerate-templates.pdf > accessed 30 May 2016.
[62] Manfred Bromba, 'On the Reconstruction of Biometric Raw Data from Template Data' (2006) <http://www.bromba.com/knowhow/temppriv.htm > accessed 30 May 2016.
[63] Arun Ross, Jidnya Shah, and Anil Jain, 'From Template to Image: Reconstructing Fingerprints from Minutiae Points' (2007) 29(4) IEEE Transactions on Patterns Analysis and Machine Intelligence 544. In a very detailed paper, the authors show which information a 'minutiae template' can reveal about a fingerprint sample. They conclude that 'the reconstructed image can be used to generate synthetic prints that can be used to compromise the security of a biometric system. If other information (…) are available in the template, then, perhaps, the original fingerprint can be reconstructed in its *entirety*.'
[64] Kai Cao and Anil Jain, 'Learning Fingerprint Reconstruction: from Minutiae to Image' (2015) 10(1) IEEE Transactions on Information Forensics and Security 104. Cao and Jain have pursued the research on the possibility to reconstruct a fingerprint image from a template and conclude that the reconstructed image is very close to the original sample, even if too perfect to fool a fingerprint expert.
[65] See Liu (n 23) and Kindt (n 23).
[66] A29WP, Opinion 4/2007 (n 36) 6.
[67] ibid 7-8.
[68] Established by art 68 GDPR.
[69] See eg, Anil Jain, Arun Ross, and Salil Prabhakar 'An Introduction to Biometric Recognition' (2004) 14(1) IEEE Transactions on Circuits and Systems for Video Technology 4.
[70] ibid; see also *Encyclopedia of Biometrics* (n 26), definition of Behavioural Biometrics, 62.

provide the same examples for physical and physiological ones: fingerprints, face, palm geometry.

### 4. Allowing or Confirming the Unique Identification of that Individual

This criterion is a key element in the legal qualification of biometric data. It describes the purposes of use of the biometric characteristics, from which biometric data are extracted. It also sets the threshold for identification applicable to biometric data as a category of personal data. It builds on an understanding of the difference of meaning between biometric identification and identification in a data protection context.

#### *a. The Different Meanings of Identification*

For the biometric community, identification has a very specific and narrow meaning. It refers to the process of establishing the identity of an individual by comparing a biometric sample with previously stored biometric templates that exist across different databases.[71] This is the 'one-to-many' matching.[72] Identity in a biometric context does not require establishing the civil or legal identity of an individual, but determining that a sample and a previously recorded template originate from the same person. Identity is established, when a match is found between a biometric characteristic and a biometric template.



Biometric identification is generally opposed to identity verification (or biometric verification). Identity verification is often called 'authentication', but this is an incorrect usage of the term according to the biometric community.[73] As observed by Kindt, authentication is used as a synonym of verification, identification and biometric recognition.[74] But because one cannot deduce the functionality to which it refers,[75] the term 'authentication' should be avoided. This is important for terminological precision, since Recital 51 GDPR mentions the term 'authentication' in opposition to 'unique identification'. This issue is further developed in the next sub-section. Verification is the process of verifying if an individual is who she or he claims to be.[76] The purpose is therefore not to establish the identity of an individual, but solely to verify it. The comparison process in that case is known as 'one-to-one' matching.[77] The biometric sample of an individual is only compared with the biometric information contained in one device, such as a smart card, an ID card, a passport, or in a single database.

Until the introduction of the concept of 'biometric data' within the scope of the data protection legislation, there was no reason to distinguish the general meaning of

[71] ISO/IEC 2382-37 (n 24), Term 37.08.03, defining biometric identification as 'process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single individual.'
[72] Opinion 3/2012 (n 8) 5.
[73] ISO/IEC 2382-37 (n 24), Term 37.08.03.
[74] Kindt (n 23).
[75] ibid 42.
[76] ISO/IEC 2382-37 (n 24), Term 37.08.02, defining biometric verification as: 'process of confirming a biometric claim through biometric comparison.'
[77] A29WP, Opinion 3/2012 (n 8) 6.

identification from its specific meaning in a biometric context. With the adoption of the new data protection framework, there is such a need. As described in sub-section 1, identification in a data protection context (meaning 'singling out') has a broader meaning than biometric identification (meaning 'establishing somebody's identity'). However, it can be argued that the function of identification through personal data encompasses the biometric identification function.

### *b. Functions of Biometric Data ("Allowing or Confirming")*

Biometric characteristics are thus used to perform biometric identification or identity verification. These two functions seem to be present in the definition of biometric data through the verbs 'allowing' and 'confirming'. Although these two verbs do not reflect the terminology used by biometric experts to describe the uses of biometric characteristics, one can infer that "allowing" refers to establishing the identity of an individual (biometric identification), whereas "confirming" refers to verifying his or her identity (identity verification). It is regrettable that the legal definition is not more rigorous and does not take into account the precise terminology used in the context of biometric recognition. As criticised by Stalla-Bourdillon, the legal definitions contained in the GDPR do not reflect technological practices.[78] In her study, Kindt has also emphasized the importance of using the correct technical terminology to understand the discussions about biometric data.[79]

On a positive note, one should observe that the current legal definition of 'biometric data' is much improved in comparison to the one originally proposed by the European Commission. The definition contained in the proposals of the Data Protection Reform Package only mentioned the function of 'biometric identification' and omitted that of 'identity verification'.[80]

### *c. Unique Identification*

The phrase 'unique identification' raises some terminological issues. Should it be understood as setting up the threshold of identification to be met by biometric data as personal data? Or should it be understood as referring to the 'biometric identification' function of biometric data? The wording of Recital 51 casts doubt on the exact meaning of this criterion.

Biometric data are defined as a legal category of personal data. It is therefore logical to look at the term 'unique identification' through the lens of the definition of personal data. From that perspective, 'unique identification' refers to the meaning of identification in a data protection context. As defined in Article 4(1) GDPR, data are personal if they relate to

[78] Sophie Stalla-Bourdillon, 'The GDPR and The Biggest Mess of All: Why Accurate Legal Definitions Really Matter…' (*blogpost on Peep Beep,* 12 April 2016) <https://peepbeep.wordpress.com/2016/04/12/the-gdpr-and-the-biggest-mess-of-all-why-accurate-legal-definitions-really-matter/> accessed 30 May 2016.
[79] Kindt (n 23) 42.
[80] European Commission, Proposal for the GDPR (n 17), art 4(11) reads as follows: "'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data."

an identified or identifiable individual. The threshold of identification is low, since an individual only needs to be identifiable. But that threshold is much higher for biometric data. As suggested by Kotschy in her interpretation of Article 2(a) of the Data Protection Directive, 'unique identification' is the 'highest degree of identification.'[81] As a consequence, biometric data must relate to an identified individual to legally qualify as biometric data. The adjective 'unique' is not defined. It could mean that biometric data have such particularities that they can 'unambiguously' identify an individual. They can, in particular, link an individual to his or her body. But it would not be accurate to say that, for this reason, biometric data are unique to each individual and allow their unique identification. From a scientific perspective, the 'uniqueness' of biometric characteristics is an assumption that forensic experts have challenged.[82] It has indeed never been scientifically demonstrated that two individuals do not have the same fingerprints.[83] In addition, the results on which the identification is performed are relative. Biometric recognition is indeed based on measurements and probabilities of similarities (or dissimilarities). The results obtained from the comparison of biometric data are subject to errors, in particular to false identification.[84] As such, biometric data cannot have the same function as a (static) unique identification number. The EDPS has advised against the use of biometric data as unique identifiers, because of the probabilistic nature of biometric technologies.[85]



Following that interpretation, an individual would only be identified if his or her biometric characteristics match previously recorded biometric data. In a case of a non-match, the individual remains unidentified. However, he or she could still be identifiable, i.e. he or she could be identified by a different entity than the data controller.[86] This is the case when biometric data can be matched with other data kept in a database different from the one consulted for comparison, especially in a scenario of identity verification. In that case, the individual would be identifiable. However, those 'biometric' data relating to an identifiable individual would not legally qualify as 'biometric data'. They would however be personal data, provided they fulfil the other conditions applicable to personal data in general.

---

[81] Kotschy (n 44) 35.

[82] For example, Mark Page, Jane Taylor, and Matt Blenkin, 'Uniqueness in the Forensic Identification Sciences: Fact or Fiction?' (2011) 206 (1-3) Forensic Science International 12; David Kaye, 'Questioning a Courtroom Proof of the Uniqueness of Fingerprints' (2003) 71 (3) International Statistical Review 521; Michael Saks, 'Forensic Identification: From a Faith-Based 'Science' to a Scientific Science' (2010) 201 (1-3) Forensic Science International 14.

[83] Simon Cole, 'Is Fingerprint Identification Valid? Rhetorics of Reliability in Fingerprint Proponents' (2006) 28(1) Law & Policy 109.

[84] For example, BioPrivacy, International Biometric Group, which developed Best Practices, see FAQs 'Are Biometrics Unique Identifiers ?' <http://www.bioprivacy.org > accessed 30 May 2016.

[85] EDPS, 'Comments on the Communication of the Commission on interoperability of European databases' [2006] <https://edps.europa.eu/sites/edp/files/publication/06-03-10_interoperability_en.pdf > accessed 30 May 2016; EDPS, 'Opinion of the European Data Protection Supervisor on the Initiative of the Federal Republic of Germany, with a view to adopting a Council Decision on the implementation of Decision 2007/…/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime' [2008] OJ C89/1.

[86] Recital 26 GDPR.

But a second meaning could be attributed to the term 'unique identification'. One can wonder if 'unique identification' should not be interpreted as referring to the 'biometric identification' function of biometric data. In Recital 51 GDPR, 'unique identification' is used in opposition to 'authentication', while clarifying the conditions under which pictures qualify as 'biometric data.' Recital 51 provides that:

> The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

The term 'authentication' is not clarified. However, it would be reasonable to consider that the EU institutions have used it as a synonym for 'verification'. In Opinion 3/2012 on developments of biometric technologies, the A29WP used verification and authentication as synonyms. In that Opinion, the A29WP defined the function of 'identity verification' as 'biometric verification/authentication'.[87] As mentioned earlier, the use of 'authentication' to refer to the functionalities of biometric systems is not accurate. However, if in Recital 51 GDPR, authentication means 'identity verification', should 'unique identification' be understood as referring to 'biometric identification'? This interpretation would be inconsistent with the legal definition of biometric data. In addition, since the notion of biometric data is approached from a legal perspective in the GDPR, the term 'unique identification' should logically refer to the threshold of identification of biometric data (being personal data) and not to their 'biometric identification' function. One could still note the inconsistency of wording (and then meaning) between Recital 51 GDPR and Article 4(14) GDPR.

### 5. Facial Images and Dactyloscopic Data as Examples

Biometric characteristics are not themselves considered to be biometric data. Only the personal data 'resulting' from their processing qualify as biometric data. Thus, it is not the face of an individual, but the images of his or her face (pictures) that would be classified as biometric data. Likewise, it is not his or her fingertip, but a fingerprint image that will be classified as biometric data. This is a logical conclusion since 'biometric data' as legally defined are first of all 'personal data'. To be protected under the data protection rules, personal data need to be, at least, part of a filing system or processed by automatic means.[88] The biometric characteristics themselves cannot be processed. Only the data generated from those characteristics can.

The legal definition of 'biometric data' gives two examples of those data: facial images and dactyloscopic data. Concerning facial images, not all the photographs will qualify as 'biometric data', but only the ones that 'allow the unique identification or authenticate' an

[87] A29WP, Opinion 3/2012 (n 8) 6.
[88] art 2(1) GDPR and art 3(1) of the Data Protection Directive.

individual will.[89] To determine whether a facial image is fit for biometric recognition, different factors or parameters should be taken into account, such as light, exposure, location or the resolution of the camera.[90] These parameters are logically not detailed in the GDPR, as they are linked to the technological developments in face recognition.

As for dactyloscopic data, the GDPR contains no reference or definition. Another legislative instrument on the cross-border exchange of DNA profiles and fingerprints to fight terrorism and crime, the Prüm Decision, provides a definition. Dactyloscopic data in the GDPR could be understood as defined in Article 2(i) of the Prüm Decision, i.e. as covering 'fingerprint images, images of fingerprint latents, palm prints, palm prints latents and templates of such images.'[91]

The analysis of the different components of the legal concept of 'biometric data' reveals that only personal data resulting from a special processing of biometric characteristics and relating to an identified individual will qualify as 'biometric personal data'. When those data uniquely identify an individual, they will benefit from the protection granted to sensitive data. This special regime is the issue addressed in the next section.



## IV. The Regime for Sensitive Data Applicable to the Processing of Biometric Data

Sensitive data (designated under the term 'special categories of data')[92] are a category of personal data that necessitate a higher degree of protection because of the consequences that their misuse would have on individuals.[93] The consequences are considered so damageable that their processing is prohibited unless an exception applies. The regime of sensitive data is defined in Article 8 of the Data Protection Directive.[94] This provision contains an exhaustive list of sensitive data, which are 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.'

The Data Protection Reform Package has added biometric data to the list of sensitive data. According to Article 9(1) GDPR, the processing of biometric data 'for the purpose of uniquely identifying a natural person' is prohibited, unless one of the exceptions set out in

[89] Recital 51 GDPR.
[90] Face recognition is based on individual's distinctive facial characteristics, for guidance on face recognition, see for example EDPS, 'Video Surveillance Guidelines' [2010], and A29WP, 'Opinion 02/2012 on facial recognition in online and mobile services' [2012] WP192.
[91] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L210/1 (Prüm Decision).
[92] art 8 of the Data Protection Directive and art 9 GDPR.
[93] A29WP, 'Advice Paper on Special Categories of Data ('Sensitive Data')' Ref. Ares (2011) 444105 [2011].
[94] art 8(1) of the Data Protection Directive reads as follows: 'Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'; art 8(2) of the Data Protection Directive provides for some exceptions to the general prohibition of processing.

Article 9(2) GDPR applies. Before the adoption of the Data Protection Reform Package, the debate around the nature of biometric data from a data protection perspective revolved around their content (i.e. whether they could reveal sensitive information) and their qualification (whether they could be considered themselves as sensitive data). This section analyses the different issues and assesses the new condition added to trigger the protection granted to sensitive data.

### 1. Debate before the Adoption of the Data Protection Reform Package

For many years, the main issue about the sensitive nature of biometric data concerned their capacity to reveal sensitive data in the sense of Article 8 of the Data Protection Directive. Among the listed sensitive data, 'data concerning health' or 'revealing racial or ethnic origin' are of particular interest when it relates to the content of biometric data. Several scientific studies on fingerprints have indeed shown that biometric data could reveal this type of sensitive data. Medical research has in particular demonstrated that the pattern of fingerprint's ridges can indicate a risk of illnesses (such as diabetes).[95] Recent studies have also found that fingerprint patterns encode information about an individual's ancestral background (ethnicity).[96]

The A29WP and the EDPS have also expressed their opinion on the topic. In Opinion 3/2012, the A29WP considered that 'some biometric data', such as facial images could reveal sensitive data relating to health condition or ethnic/racial origin, but in that Opinion the Working Party did not qualify biometric data as sensitive data.[97] As for the EDPS, in several opinions relating to the processing of biometric data for passports and travel documents, it viewed biometric data as being 'highly'[98] or 'inherently sensitive,'[99] because of their characteristics and not because of the sensitive information they could reveal. Based on those opinions, the Advocate General Mengozzi in Case C-291/12 on the validity of the Passport Regulation (Council Regulation 2252/ 2004) stated that biometric data are sensitive data by nature.[100] On this specific point, the European Court of Justice did not follow his opinion. The Court, however, ruled that 'biometric data' are personal data because 'they objectively contain unique information about individuals which allows those individuals to be identified with precision.'[101]

On the formats of biometric data, the A29WP has not said much, although, in 2003, it did state that it considered that images are more susceptible to reveal sensitive data than the

[95] In particular Henry S Kahn et al, 'A Fingerprint Marker from Early Gestation Associated with Diabetes in Middle Age: the Dutch Hunger Winter Families Study' (2009) 38(1) International Journal of Epidemiology 101.
[96] Nichole A Fournier and Ann H Ross, 'Sex, Ancestral, and Pattern Type Variation of Fingerprint Minutiae: a Forensic Perspective on Anthropological Dermatoglyphics' (2015) American Journal of Physical Anthropology, online access 23 September 2015.
[97] A29WP, Working Document on Biometrics (n 7) 10.
[98] EDPS, 'Opinion of 23 March 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas' (COM (2004) 835 final), Section 3.4.2 Specific Nature of Biometrics [2005] OJ L181/13.
[99] EDPS, Opinion of 19 October 2005 on the three SIS II proposals, Section 4.1 Biometrics [2005] OJ C91/38.
[100] C-291/12, *Michael Schwarz v Stadt Bochum* [2013] EU:C:2013:401, Opinion of AG Mengozzi, para 52.
[101] C-291/12, *Michael Schwarz v Stadt Bochum* [2013] EU:C:2013: 670.

templates themselves.[102] Its analysis was based on the beliefs that a biometric image could not be regenerated from a biometric template.[103] In Opinion 3/2012, the Working Party did not amend its position, although by that time it was known that biometric templates could be partially reversible. Having said this, it is not sure from a scientific point of view that sensitive information can be derived from biometric templates. According to the state of the art in biometric recognition, a biometric image can partially be reconstructed from a biometric template.[104] From that reconstructed image, and in the absence of research on this issue,[105] it is however not certain that sensitive information can be identified.

In legal literature, the analysis by Yue Lui on the specific nature of biometric data provides some interesting insights. Based on a decision of the Norwegian Data Protection Authority on the use of CCTV in buses, Yue Lui explains that some view biometric data as 'carriers' of personal data and not as 'sensitive data' themselves. However, they become sensitive in case they are 'processed with the intention or consequence of generating sensitive information, such as health, genetic or racial information.'[106] Thus, it is the context of the use of biometric data that would condition the application of the regime of sensitive data. At the same time, Yue Lui states that she is not convinced by this reasoning. She explains that the status of biometric data should not be linked to the sensitive data they can reveal, but to their own characteristics. According to Yue Lui, because biometric data can be used as 'relatively unique and universal 'key data' for getting all kinds of personal information,'[107] they should be considered "as 'sensitive personal data' in general."



### 2. Purpose of Processing as a New Condition to Apply the Regime of Sensitive Data

Discussions on the specific nature of biometric data were revived during the public consultations that preceded the launch of the proposals of the new data protection framework. Between 2009 and 2011, the European Commission consulted national authorities and stakeholders on the future of the data protection regime.[108] Several of these mentioned the issue of the specific nature of biometric data and suggested adding them to the list of sensitive data.[109] However, in the proposals on the Data Protection

[102] A29WP, Working Document on Biometrics (n 7) 10.
[103] ibid, 'whether a processing contains sensitive data is a question of appreciation linked with the specific biometric characteristic used and the biometric application itself. It is more likely to be the case if biometric data in the form of images are processed, since in principle the raw data [understood here as image] may not be reconstructed from the template.'
[104] Cao and Jain (n 64).
[105] To the best of this author's knowledge.
[106] Yue Lui, *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics* (Routledge 2012), 120.
[107] ibid 121.
[108] European Commission (n 16).
[109] eg answers from Datatilsynet, the Norwegian Data Protection Authority <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/datatilsynet_en.pdf> accessed 30 May 2016; or from Privacy International <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/pi_en.pdf> accessed 30 May 2016.

Reform Package, the European Commission only added 'genetic data' to the list.[110] It was instead the European Parliament that added them to the list of sensitive data when it voted on the proposals.[111] In the adopted texts, biometric data have been upgraded to the category of sensitive data, under the condition that they 'uniquely identify' an individual. It is therefore the purpose of the processing ('unique identification') that will trigger the regime applicable to sensitive data.

As explained in the previous section, 'unique identification' is also used as a criterion to qualify specific personal data as 'biometric data.' Contrary to the other types of personal data listed in the category of sensitive data, 'biometric data' are not treated as sensitive by nature but become sensitive as the result of their use.

#### *a. Purpose of Biometric Data Processing*

It is therefore the purpose of biometric data processing that determines the application of the regime of sensitive data. The purpose is defined as 'uniquely identifying an individual.' As per the analysis made in the previous section, biometric data resulting from both biometric identification (establishment of the identity) and identity verification should qualify as sensitive data, provided they relate to an identified individual. Still, a doubt persists because of the ambiguous wording of Recital 51 GDPR.[112] If 'allowing the unique identification' refers to the biometric identification function and 'allowing the authentication' means 'identity verification,' biometric data used for identity verification (such as passport/ID verification) would be excluded from the scope of sensitive data. But, as already observed, Recital 51 is inconsistent with Article 4(14) GDPR that defines the legal concept of biometric data. The definition distinguishes the function of 'allowing the unique identification' (which covers the biometric identification function) from that of 'confirming the unique identification' (which covers the identity verification function). Unique identification is then understood as the identity of an individual. Following the definition, biometric data used for biometric recognition (identification and verification) and linked to an identified individual benefit from the status of sensitive data.

It is difficult to reconstruct the intention of the EU legislator: the notion of 'biometric data' was not included in the list of sensitive data contained in the proposals of the Data Protection Reform Package. Likewise, not much can be found in the discussions on the proposals either. The criterion of the purpose of the processing was indeed added very

[110] European Commission (n 17), Art 9(1) of the proposed GDPR reads as follows: 'the processing of personal data revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.'

[111] European Parliament, legislative resolution on the proposal for a GDPR (COM (2012) 0011-C7-0025/2012-2012/0011(COD)), Art 9(1) of the amended proposal of GDPR reads as follows: 'the processing of personal data, revealing race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership and activities, and the processing of genetic or biometric data or data concerning health or sex life, administrative sanctions, judgments, criminal or suspected offences, convictions or related security measures shall be prohibited.'(P7_TA(2014)0212)[2014].

[112] Recital 51 GDPR.

late in the trilogue negotiations on the Data Protection Reform Package:[113] neither the resolutions on the proposals adopted by the European Parliament nor the political agreements reached by the Council mentioned the criterion. It can however be found in the draft version of modernisation of Convention 108.[114] The draft Convention is completed with a Draft Explanatory Report. The 2013 Draft mentions that 'solely the processing which will lead to the unique identification of an individual' is 'to be considered as sensitive.'[115] The Draft also contains the example of photographs, reproduced in Recital 51 GDPR, and provides the conditions under which pictures should constitute biometric data. The trilogue at the EU level seems to have aligned the texts of the Data Protection Reform Package with the draft revision of Convention 108.

#### *b. Sensitive Data by Reason of their Nature*

It is questionable whether biometric data should not have been treated 'sensitive data' by reason of their nature and not because of their purpose of use. In the original proposals of the Data Protection Reform Package, the European Commission did not add biometric data to the list of sensitive data, but only genetic data.[116] It justified the addition of 'genetic data' by reference to the ruling of the European Court of Human Rights (ECtHR) in *S & Marper v UK*.[117] In that case, relating to the retention of DNA samples, fingerprints and cellular samples of persons suspected but never convicted, the Court ruled on the sensitive nature of DNA information. It found that their sensitivity was linked to their characteristics – i.e. the possibility that DNA information could reveal ethnic origin[118] and family genetic makeup.[119] The ECtHR did not follow the same approach and reasoning for fingerprints, as the Court considered 'common ground that fingerprints do not contain as much information as either cellular samples or DNA profiles.'[120] The judgement was rendered in 2008 when fingerprint recognition technologies were less developed. Since that time, some scientific studies have shown that sensitive information, such as ethnicity[121] and illnesses[122] can possibly be derived from fingerprints. It can be argued

[113] The political agreements reached by the Council on the text of the General Data Protection Regulation in June 2015 and on the text of the Directive on data protection for law enforcement purposes did not mention biometric data in the list of sensitive data.
[114] Council of Europe, Consultative Committee of Convention 108 for the protection of Individuals with regard to automatic processing of personal data (ETS No. 108), Propositions of modernisation adopted by the 29th Plenary meeting (T-PD(2012)4Rev4) [2012]; the modernisation process started in 2011 and is still ongoing.
[115] Council of Europe, Bureau of the Consultative Committee of Convention 108, 'Draft Explanatory Report of the Modernised Version of Convention 108', T-PD-BUR (2013) 3ENrev, para 56.
[116] European Commission, proposal for the GDPR (n 17) and proposal for the Directive on law enforcement (n 18).
[117] See *S and Marper v United Kingdom* [2008] ECHR 1581, and European Commission, 'Impact Assessment accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', Brussels, 25 January 2012, SEC (2012), 55.
[118] *S and Marper v UK,* para 76.
[119] ibid para 103.
[120] ibid para 78.
[121] A29WP, Opinion 02/2012 (n 90); Fournier et al (n 96).
[122] Kahn et al (n 95).

that, if the ECtHR were to examine the issue now, the Court ought to take into account the state of the art in fingerprint recognition and question whether 'biometric data' should not be treated as sensitive data because of their nature.[123]

The regime of sensitive data contained in the GDPR is quite similar to the one set in the Data Protection Directive. The general rule is the prohibition of processing sensitive data unless one of the exceptions listed in Article 9(2) GDPR applies.[124] The grounds for processing sensitive data are broadly similar to those under the Data Protection Directive, with some additions made in the area of health. In application of Article 9(4) GDPR, Member States have the possibility to adopt other conditions or stricter rules to allow their processing.[125]

## V. Conclusions

The long-awaited provisions of the new data protection framework bring some certainties on the status of biometric data. They define the concept of biometric data taking into account the technical processing through which biometric characteristics are transformed into data. Equally importantly, the new provisions also grant the status of sensitive data to biometric data. But those certainties might only be illusory.

The legal definition of biometric data from a data protection perspective sets the conditions under which personal data can qualify as 'biometric data' and not the conditions under which 'biometric data' become personal data. The concept of biometric data is defined as a type of personal data. The definition combines the technical criteria of biometric data (e.g. the technical processing of biometric characteristics) with legal criteria applicable to personal data (e.g. the function of 'unique identification). However, the definition lacks preciseness when it addresses the functions of 'biometric recognition'. The terminology used by the biometric community to describe these functions, i.e. biometric identification and identity verification, is not re-used in the legal definition of biometric data. Instead, one should deduce that the verbs 'allowing' and 'confirming' respectively refer to the functions of 'biometric identification' and 'identity verification'. As for the criterion of 'unique identification', it sets the threshold of identification applicable to biometric data. Contrary to 'generic' personal data, biometric data must relate to an identified individual. The other 'biometric data', i.e. those that relate to an

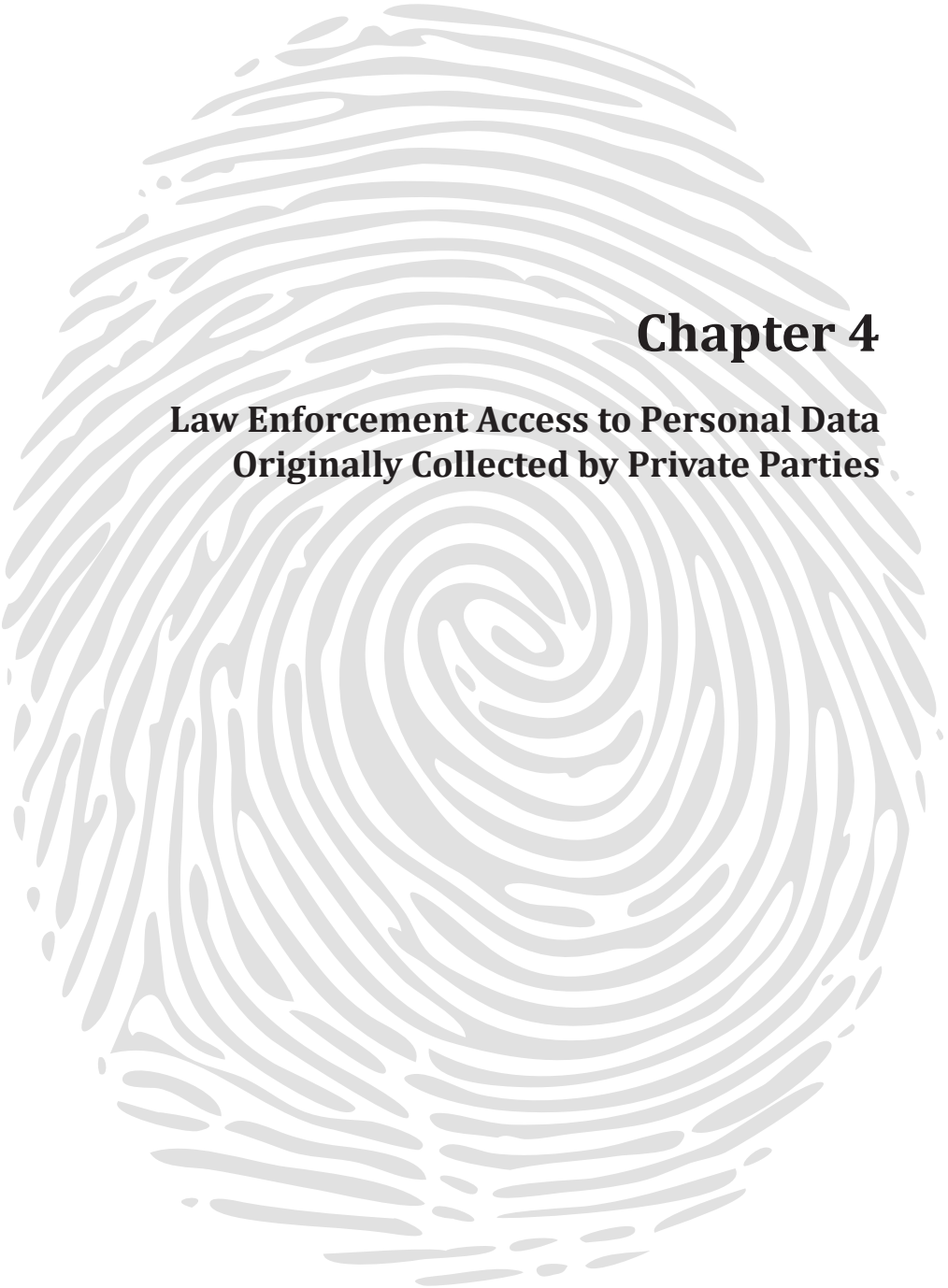
[123] It could also be argued that biometric data and genetic data share several similarities from a data protection perspective: they both rely on permanent physiological characteristics for individual recognition and they can both reveal sensitive information. In addition, several national data protection laws (Slovenia, Slovakia) already include genetic data in the broader category of biometric data. Some authors (eg Kindt) support such a distinction on the ground that genetic data cannot be used for automatic recognition. But scientific research in the field (Jain) anticipates that 'in the near-future' DNA-profile matching might be done in real-time or at least within a few minutes.

[124] art 9(2) GDPR provides for ten exceptions including explicit consent, legal obligations of the controller in the field of employment or social security and protection of the vital interests of the data subjects or of another individual.

[125] art 9(4) GDPR reads as follows: 'Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.'

identifiable individual, do not legally qualify as biometric data, but can still be considered as personal data if they fulfil the other criteria applicable to personal data. The new data protection framework creates a new legal category of biometric data, which could be qualified of 'biometric personal data' to reflect their nature as personal data.

The new provisions also add the category of biometric data to the list of sensitive data, but not by virtue of their nature. In the new regime, the purpose of processing (that is, to uniquely identify an individual) determines the application of the regime of protection. This condition is connected to the threshold of identification applicable to biometric data. However, taking into account the state of the art in biometric technologies, it is debatable whether biometric data should rather have been treated as sensitive by nature.



# Chapter 4

## Law Enforcement Access to Personal Data Originally Collected by Private Parties

## *Chapter 4: Law Enforcement Access to Personal Data Originally Collected by Private Parties*

*Missing Data Subjects' Safeguards in Directive 2016/680?* [*]

**Abstract:**
*Access by law enforcement authorities to personal data initially collected by private parties for commercial or operational purposes is very common, as shown by the transparency reports of new technology companies on law enforcement requests. From a data protection perspective, the scenario of law enforcement access is not necessarily well taken into account. The adoption of the new data protection framework offers the opportunity to assess whether the new 'police' Directive, which regulates the processing of personal data for law enforcement purposes, offers sufficient safeguards to individuals. To make this assessment, provisions contained in Directive 2016/680 are tested against the standards established by the ECJ in Digital Rights Ireland and Tele2 Sverige on the retention of data and their further access and use by police authorities. The analysis reveals that Directive 2016/680 does not contain the safeguards identified in the case law. The paper further assesses the role and efficiency of the principle of purpose limitation as a safeguard against repurposing in a law enforcement context. Last, solutions to overcome the shortcomings of Directive 2016/680 are examined in conclusion.*

### I. Introduction

Law enforcement authorities around the globe have a growing appetite for personal data held by private parties and initially collected for a purpose different than law enforcement. Many examples can illustrate this trend: the huge amount of law enforcement requests made to high-tech companies at global level,[1] the case of the transfer of passenger name

[*] Article published in the *Computer Law & Security Review*, volume 34, issue 1, February 2018, pages 154-165. The author would like to thank Prof Jeanne Mifsud Bonnici and Prof Laurence Gormley for their valuable comments on an earlier draft, Christina Angelopoulos for kind suggestions as well as the anonymous reviewers; any error or omission is however the sole responsibility of the author.

[1] For the first half-year of 2016, Microsoft reported more than 25,000 law enforcement requests to disclose content, subscriber data or transactional data at global level, see <https://www.microsoft.com/about/csr/transparencyhub/lerr > compare with Apple's and Google's reports for the same period, available at respectively <images.apple.com/legal/privacy/transparency/request-2016-H1-en.pdf> and <https://www.google.com/transparencyreport/userdatarequest/countries/>
See also, Oleg Afonin, 'Government Request Reports: Google, Apple and Microsoft ' (*ElcomSoft* blog, 16 January 2017) <https://blog.elcomsoft.com/2017/01/government-request-reports-google-apple-and-microsoft/>
(all the above websites were accessed on 1 August 2017).

record data (air traveller data) to police authorities,[2] or the retention of telecommunications data by Internet Service Providers (personal data retention) for further use by law enforcement authorities.[3]

Other examples for which the number of requests for access might not be publicly known could follow. Given their characteristics, one could think of the value that some types of personal data have for law enforcement authorities. This is the case of biometric data (such as fingerprints), which have been used for many decades by police authorities to identify individuals.[4] Private parties rely more and more on biometric data to control access to buildings, IT systems or applications. Several social media companies, e.g. Facebook, have even constituted biometric databases based on the facial images of their users. In Europe, Facebook stopped facial recognition in 2012, whereas in the USA the company is still collecting such personal data.[5] Of course, Facebook has more personal data than its users' facial images: it might also hold names (real or alias), date of birth, addresses, phone numbers, and any kind of personal information a user is willing to provide under their profile. All these personal data, including biometric data, constitute valuable information for criminal intelligence and criminal investigation.[6] Criminal intelligence is a form of surveillance carried out by law enforcement authorities to gather information about crime or criminal activities before their occurrence or to establish their occurrence.[7] It differs from criminal investigation, which corresponds to a procedural stage in relation to concrete criminal activities.[8] These two activities are covered in this paper.



[2] On the Passenger Name Record, see International Civil Aviation Organization, 'Guidelines on Passenger Name Record (PNR) Data', Section 2.1. (1st edn, ICAO 2010) <https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf> accessed 1 August 2017; see also Directive 2016/681 of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offence and serious crime [2016] OJ L119/132.

[3] See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54.

[4] eg Simon A Cole, *Suspect Identities: A History of Fingerprinting and Criminal Investigation* (Harvard Press University 2001).

[5] It should be noted that the collection, storage, retention and subsequent use of facial images by Facebook have been challenged in Illinois for the lack of informed consent from the individuals concerned, see Class Action Complaint for violations of the Illinois Biometric Information Privacy Act <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1971&context=historical > accessed 1 August 2017.

[6] See for example, Press Association, 'Facebook receives nearly 2,000 data requests from UK police' *The Guardian* (11 April 2014) <https://www.theguardian.com/technology/2014/apr/11/facebook-2000-data-requests-police> accessed 1 August 2017.

[7] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L386/89; see Art 2 (c) that reads as follows: 'crime and criminal activities with a view to establish whether concrete criminal acts have been committed or may be committed in the future.'

[8] Council Framework Decision 2006/960/JHA, see Art 2 (b) that reads as follows: 'a procedural stage within which measures are taken by competent law enforcement authorities or judicial authorities, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts.'

From a data protection perspective, the obvious questions that arise from this scenario are which legal framework applies to the case of law enforcement access to personal data held by private parties, and whether that framework provides sufficient safeguards to data subjects. The adoption of a new data protection framework at EU level constitutes an excellent opportunity to assess the rules applicable to the scenario at that level. Adopted in April 2016, the new data protection framework is composed of a General Data Protection Regulation (Regulation 2016/679 or GDPR)[9]- replacing the Data Protection Directive -[10] and of a Directive on the protection of personal data processed for law enforcement purposes (Directive 2016/680 or the 'police' Directive).[11] The 'police' Directive replaces the Council Framework Decision 2008/977/JHA adopted under the previous pillar structure.[12] Directive 2016/680 defines the rules applicable to the processing of personal data for law enforcement purposes and more specifically for the purposes of 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.'[13] The phrase 'law enforcement purposes' should therefore be understood, in the context of this article, as referring to the purposes regulated in Directive 2016/680. The Directive does not explicitly define the different purposes but relies on national laws. Criminal investigation purposes as well as criminal intelligence purposes can therefore fall within the scope of Directive 2016/680.

Against this background, the next section, Section 2, addresses the applicability of both the GDPR and the 'police' Directive to the scenario described in this article: provisions contained in the GDPR govern the initial processing of personal data by private parties, whereas rules set out in the 'police' Directive cover the further processing of the data by law enforcement authorities. After having established that the further processing of personal data falls within the scope of Directive 2016/680, Section 3 analyses the rules of that Directive to determine whether they lay down sufficient safeguards to protect individuals whose personal data are accessed by law enforcement authorities. The rules are assessed against the standards established by the European Court of Justice (ECJ) in two related judgments on the retention of personal data. *Digital Rights Ireland*[14] and *Tele2*

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
[11] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.
[12] Before the entry into force of the Lisbon Treaty, the EU policy areas were divided into three pillars. The first pillar was composed of the economic communities whereas the third one regrouped police and judicial matters in criminal matters, see eg Catherine Barnard and Steve Peers, *European Union Law* (OUP 2014).
[13] art 1 of Directive 2016/680.
[14] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* [2014] ECLI:EU:C:2014:238.

*Sverige*[15] are particularly relevant to the scenario of law enforcement access to personal data held by private parties as they both relate to the retention of data for later access and use by law enforcement and national securities authorities. Section 3 discusses the two cases and extracts the relevant findings in an attempt to apply them to the provisions of Directive 2016/680. Finally, Section 4 addresses the issue of the change of initial purpose and critically assesses the principle of purpose limitation as a safeguard against abuses or misuses.

## II. Applicable Legal Instrument: the GDPR or the 'Police' Directive?

This section considers which legal instrument is applicable to the scenario of law enforcement access to personal data initially collected by private parties for a non-law enforcement purpose. It provides some background on the negotiations of the 'police' Directive and explains how the diverging positions of the EU institutions on the issue of law enforcement access have resulted in the adoption of complicated recitals on the topic. It concludes that both the GDPR and the 'police' Directive apply to the scenario.


### 1. Positions of the EU Institutions: Between Hesitation and Divergence

The GDPR and the 'police' Directive build a bridge between them on the issues of the further processing of personal data for a purpose falling under the scope of each other's instrument. Recital 11 of Directive 2016/680 evokes the scenario of personal data collected for a law enforcement purpose and further processed for a non-law enforcement purpose. In that case, the further processing is covered by the GDPR. Recital 19 of the GDPR describes the other-way around scenario and provides for the applicability of Directive 2016/680 to the further processing by law enforcement authorities of personal data initially collected for a non-law enforcement purpose. However, both scenarios are worded in a complicated manner.[16] It could be that the wording results from the divergent approaches defended by the EU institutions during the negotiations of the new data protection framework, and in particular of the draft 'police' Directive.

In January 2012, the European Commission published a proposal for a 'police' Directive that did not contain any reference to the scenario of law enforcement access to personal data collected by third parties. Yet, a few months before, Statewatch, a civil liberties organisation, leaked a draft version of the proposal which included an article containing procedural safeguards specific to the access by law enforcement authorities to personal

[15] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and others* [2016] ECLI:EU:C:2016:970.

[16] Recital 11 of Directive 2016/680 refers to 'other bodies or entities entrusted by Member State law to exercise public authorities and public powers for the purpose of this Directive [i.e. Directive 2016/680]' and explains that 'where such a body or entity processes personal data for purposes other than for the purposes of this Directive [i.e. Directive 2016/680], Regulation (EU) 2016/679 applies'; whereas Recital 19 of Regulation 2016/679 specifies that 'personal data processed by public authorities under this Regulation should, when used for those purposes, [which are the purposes of prevention, investigation, detection or prosecution of criminal penalties] be governed by a more specific Union legal act, namely Directive (EU) 2016/680.'

data initially collected for purposes other than law enforcement.[17] Those very detailed safeguards comprised: (a) the persons entitled to have access to the personal data under the condition that the data met a 'reasonable ground standard'; (b) a written request referring to the legal basis on which the request was made; and (c) the adoption of 'appropriate safeguards' defined by the Member States, which could include, among others, a prior judicial review of the request.[18] This draft never saw the light of day and the official proposal for the 'police' Directive did not contain any specific provisions on that issue.

During the negotiations on the proposal for the 'police' Directive, the European Parliament brought the issue back on the table and proposed a new article on 'law enforcement access to personal data collected for a different purpose.'[19] In that amendment, the usage of the personal data initially collected for a different purpose could only be limited to 'investigation' or 'prosecution of criminal offence'.[20] However, the other institutions did not endorse the amendment. With the exception of one delegation, the Council did not support the amendment and adopted a political agreement on the proposal without such a provision.[21] As for the European Commission, it stated that it was not able to fully endorse the amendment. It argued that there was a risk of confusion –without specifying on which topic- and of non-compliance with international agreements, such as the Passenger Name Record and the Terrorist Tracking Programme.[22] Those arguments are very surprising and not very convincing: the Commission justified its position by referring to controversial agreements providing foreign law enforcement authorities (mainly US ones) access to EU citizens' personal data.

[17] See draft version of a 'proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' ('Police and Criminal Justice Data Protection Directive') version 34, 29 November 2011, see art 4 (2)(a)-(c)
< http://www.statewatch.org/news/2011/dec/ep-dp-leas-draft-directive.pdf > accessed 1 August 2017.
[18] art 4 (2)(c) of the leaked draft version of a proposal for a 'Police and Criminal Justice Data Protection Directive.'
[19] European Parliament legislative resolution of 12 March 2014 on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM (2012) 0010 – C7-0024/2012- 2012/0010(COD))(Ordinary legislative procedure: first reading), Art 4a.
[20] ibid.
[21] See Council, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, FN 130, Austrian delegation, LIMITE doc. no 7740/15, 14 April 2015.
[22] Extracted from the leaked 'Commission position on EP amendments on 1st reading': 'have or risk having the effect of prohibiting lawful access by competent law enforcement authorities to PNR [Passenger National Register], TFTP [Terrorist Finance Tracking Programme] or other relevant personal data as provided for under international agreements concluded by the Union or existing or proposed legal instrument'; TFTP is an 'Agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program' [2010] OJ L8/11, and Council Decision on the agreement [2010] OJ L195/3.

In fine, the adopted provisions contained in the GDPR and the 'police' Directive seem to reflect the divergence of the EU institutions on this issue.

### 2. Two Sets of Rules Governed by Two Different Instruments

The scenario of law enforcement access to personal data generated by private parties for a non-law enforcement purpose can be split into the 'initial purpose of collection,' subject to the GDPR, and the 'purpose of further processing', governed by Directive 2016/680.

In the scenario under review, the *initial purpose of data collection* mostly relates to customer data collected by private parties. Provided it complies with the conditions set out in Article 2(1) GDPR, the initial purpose of collection is subject to the rules contained in the GDPR.[23] The collection of personal data is also an example of processing activities explicitly covered by the GDPR.[24]

The *further processing* of personal data held by private parties falls within the scope of Directive 2016/680 if the data are further processed for a law enforcement purpose. As already explained, on this issue, Recital 19 GDPR builds a bridge between the GDPR and Directive 2016/680. One could still regret that the applicability of the 'police' Directive is only mentioned in a non-binding provision. Law enforcement access to and use of personal data should therefore fall in the category of data processing operations, as set out in Article 3(2) of Directive 2016/680.



A discussion can ensue on the exact meaning of the term 'access'. Access is not included in the list of processing operations given as examples in Article 3(2) of Directive 2016/680.[25] The term is also ambiguous: it can refer to different processing operations ('consultation' or 'disclosure') involving different actors (private parties providing the access to the data or law enforcement getting access to them) and be thus subject to different rules. If disclosure of personal data by private parties to law enforcement authorities seems to fall within the remit of the GDPR, 'consultation' of those data by law enforcement authorities could be subject to diverging interpretations. One could argue that 'consultation' by law enforcement authorities is nothing more than 'making available' the personal data to law enforcement authorities and thus disclosure. But at the same time, 'consultation' could also be considered a processing subject to the 'police' Directive if personal data are, for instance, consulted by law enforcement authorities in the context of a criminal investigation. Approaching the term from its terminological and operational meaning might be too simplistic to determine which legal instrument applies.

[23] art 2(1) GDPR defines the scope of the Regulation as follows: 'This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.'
[24] art 4(2) GDPR defines the term 'processing' and provides as examples '***collection***, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' (emphasis added).
[25] Processing is defined in identical terms in art 3(2) Directive 2016/680 and art 4(2) GDPR; consultation and disclosure are both examples of processing activities.

Trying to understand the meaning of 'access' is not a rhetorical issue since it has been mentioned in the case law of the ECJ on data retention. However, one cannot but notice that the case law does not bring much clarity on the status and meaning of 'access'. In case C-301/06 relating to the validity of the legal basis on which the Data Retention Directive had been adopted,[26] the Court found that the Data Retention Directive regulated the retention of personal data but not their access or use by law enforcement authorities.[27] By contrast, in *Digital Rights Ireland* and more clearly in *Tele2 Sverige* - both described at length in the next section - the Court viewed the operation of law enforcement access to the retained data as an accessory to the retention of personal data and extended the application of EU law to the operation of access.[28] The Court justified it through the link existing between the purpose of retention of the data and their use.[29] As noted by Woods, the Court refused to make a distinction between retention and access to the retained data and therefore to exclude access from the scope of EU law.[30] It should be observed that *Digital Rights Ireland* and *Tele2 Sverige* were decided before the adoption of the new data protection framework. Under the new rules, access by law enforcement authorities for a law enforcement purpose should fall within the scope of Directive 2016/680 and be distinct from retention of data processed for a non-law enforcement purpose. In any case, in this paper, what matters is the purpose for which privately held personal data are further accessed and not whether access means 'consultation' by law enforcement authorities or 'disclosure' by private parties.

As described in this section, the GDPR applies to the initial purpose of collection, whereas the 'police' Directive applies to the further processing of the same data by law enforcement authorities. Although both texts acknowledge the scenario and determine the instrument applicable thereto, they do not contain specific rules applicable to the law enforcement access to personal data collected for a different purpose. Yet Opinion 03/2015 of the Article 29 Data Protection Working Party (A29WP)[31] on the proposal for a 'police' Directive recommended: 'any processing for a purpose different than the specific one for which the data was originally processed should always have its own legal basis

[26] Case C-301/06, *Ireland v European Parliament and Council* [2009] ECLI:EU:C:2009:68.
[27] Case C-301/06, para 80; see also Art 4 Directive 2006/24.
[28] *Tele2 Sverige* (n 15) para 76.
[29] *Tele 2 Sverige* (n 15) para 79: 'since data is retained only for the purpose, when necessary, of making that data accessible to the competent national authorities, national legislation that imposes the retention of data necessarily entails, in principle, the existence of provisions relating to access by the competent national authorities to the data retained by the providers of electronic communications services'; see also Opinion of A.G. Saugmandsgaard ØE in *Tele2 Sverige*, para 125: 'the *raison d'être* of a data retention obligation is to enable law enforcement authorities to access the data retained, and so the issue of the retention of data cannot be entirely separated from the issue of access to that data.'
[30] Lorna Woods, 'Data Retention and National Law: the ECJ Ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)' (*EU Law Analysis*, 21 December 2016) blogpost <http://eulawanalysis.blogspot.nl/2016/12/data-retention-and-national-law-ecj.html> accessed 1 August 2017.
[31] The A29WP is an independent advisory body to the European Commission on data protection matters <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083> accessed 1 August 2017.

including clear and specific safeguards.'[32] If it is established that the further processing for a law enforcement purpose of personal data held by private parties has a legal basis,[33] one can still wonder if Directive 2016/680 contains clear and specific safeguards to ensure the protection of individuals whose personal data are accessed. This issue is addressed in the next section.

## III. Existence of 'Substantive and Procedural' Safeguards in Directive 2016/680?

Besides facilitating the free movement of personal data in the area of law enforcement, Directive 2016/680 aims at ensuring the same level of protection of individuals' rights through the EU.[34] According to Recital 26 of Directive 2016/680, safeguards are an element of fair processing that should ensure that individuals are able to exercise their rights in a law enforcement context. This section will assess whether the provisions of Directive 2016/680 provide sufficient safeguards for the protection of individuals whose personal data initially collected by private parties are accessed by law enforcement authorities. To make this assessment, the paper builds on the 'standards' established by the European Court of Justice in its jurisprudence on data retention, i.e. in *Digital Rights Ireland*[35] and *Tele2 Sverige*[36]. The first case relates to the EU data retention framework, i.e. the Data Retention Directive (or Directive 2006/24), the second one to national data retention frameworks (the Swedish and UK frameworks) as described below.


### 1. Preliminary Remarks on the Use of *Digital Rights Ireland* and *Tele2 Sverige* as Benchmark

The two judgments are relevant to the scenario of law enforcement access even if they relate to slightly different situations. Indeed, in *Digital Rights Ireland* and *Tele2 Sverige*, the laws at stake cover traffic data collected by telecoms operators for their own usage and retained to be accessed (and further used) by law enforcement authorities. The laws impose an obligation to retain the data. By contrast, in the scenario under consideration, personal data are collected by private parties for their own use (or at least for a non-law enforcement purpose) and are then accessed by law enforcement authorities. Private parties are under no obligation to retain personal data for law enforcement access, they simply make the data available upon request. This is an important precision since the scenario under review does not relate to mass collection or mass retention of personal data. To illustrate it, one could think of the situation where an employer collects his

[32] A29WP, 'Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' [2015] WP233.
[33] Recital 19 GDPR.
[34] Recitals 7 and 15 Directive 2016/680.
[35] *Digital Rights Ireland* (n 14).
[36] *Tele2 Sverige* (n 15).

employees' fingerprints to give them access to secured buildings.[37] A criminal offence is then committed on the work premises. The police authorities request access to the biometric data files held by the employer to compare them with the biometric data found on site. In that specific scenario, what matters are the rules applicable to law enforcement authorities to get access to those data. However, despite the differences between the scenarios, the ECJ's rulings in *Digital Rights Ireland* and *Tele2 Sverige* also cover the issue of law enforcement access to the retained data in addition to the issue of data retention itself. It is precisely the way the ECJ approaches the issue of access that is relevant in the context of this paper.

There is also enough evidence to believe that the findings of *Digital Rights Ireland* and *Tele2 Sverige* apply to legislative measures beyond metadata retention.[38] The European Parliament and the European Commission have both addressed the issue of the impact of the *Digital Rights Ireland* judgment on other EU legislation. Prior to the adoption of the 'police' Directive, the legal service of the European Parliament delivered an opinion on the consequences of *Digital Rights Ireland*.[39] Since at that time, national legislation on the processing of personal data for law enforcement authorities fell outside the scope of EU law,[40] it considered that the rules on law enforcement access to and use of personal data collected for a different purpose were not necessarily impacted by the judgment. However, it also acknowledged that its position would be different if and when the proposal for a 'police' Directive would be adopted.[41] A few months later, the European Parliament asked the European Commission to assess the possible impact of *Digital Rights Ireland* on the proposed Passenger Name Record (PNR) Directive.[42] In its answer to the European Parliament, the European Commission opined that the judgment set up a framework to assess EU legislation on 'the general collection and processing for law enforcement

[37] eg Guidelines by the Irish Data Protection Commission on 'Biometrics in the Workplace' <https://www.dataprotection.ie/docs/Biometrics-in-the-workplace/m/244.htm> accessed 1 August 2017; position of the French data protection authority (CNIL) on the use of biometric systems to control access to working places <https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail> accessed 1 August 2017.

[38] See also Franziska Boehm and Mark Cole, 'Data Retention after the Judgement of the Court of Justice of the European Union' (30 June 2014), in which the authors assess the impact of the DRI judgment on other Data Retention Measures
<https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf > accessed 1 August 2017.

[39] Legal Service of the European Parliament, leaked document, legal opinion of 22 December 2014 'LIBE-Questions relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* - Directive 2006/24/EC on data retention - Consequences of the judgment' [2014] para 80
<http://www.statewatch.org/news/2015/apr/ep-ls-opinion-digital-rights-judgment.pdf> accessed 1 August 2017.

[40] The only data protection framework applicable in the context of law enforcement was the Council Framework Decision 2008/977/JHA that only covered cross-border processing for law enforcement purposes, see Recital 7 and art 1 of Council Framework Decision 2008/977/JHA.

[41] Opinion of the European Parliament (2014), footnote 62 reads as follows: ' it [i.e. the draft Directive] will bring important changes to the Union's data protection law in the area of criminal law, in comparison to the act currently in force, i.e. Council Framework Decision 2008/977/JHA.'

[42] European Parliament, 'Resolution of 11 February 2015 on anti-terrorism measures' (2015/2530 (RSP)) [2015] Point 13 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0032+0+DOC+XML+V0//EN > accessed 1 August 2017.

purposes of personal data of individuals.'[43] The Commission acknowledged in particular that the findings of the *Digital Right Ireland* case should be taken into account in the assessment of the proposal for a PNR Directive.[44]

As for *Tele2 Sverige*, the judgment assesses the impact and application of the *Digital Rights Ireland* judgment to national data retention regimes. Because of the scope of Directive 2016/680,[45] it can be strongly asserted that its findings apply to national legislation relating to the collection of personal data by third parties and to their further processing by law enforcement authorities.

### 2. The Benchmark set by *Digital Rights Ireland* and *Tele2 Sverige*

The Data Retention Directive was 'struck down' by the ECJ in *Digital Rights Ireland*; whereas national data retention measures still in place (Sweden) or adopted after the invalidation of the Directive (UK) were declared incompatible with EU law in *Tele2 Sverige*. These two cases have a strong connection. Following the invalidation of the Data Retention Directive, national measures on data retention still had to be compliant with EU law, and in particular, with the e-privacy Directive (or Directive 2002/28/EC) adopted before the Data Retention Directive. Article 15(1) of that Directive expressly allows Member States to adopt data retention measures under specific conditions. It is against that provision that the ECJ had to determine the compliance of the Swedish and UK measures in *Tele2 Sverige*.



In *Digital Rights Ireland*, two national jurisdictions, the High Court of Ireland and the Verfassungsgerichtshof (Austrian Constitutional Court), brought a request for preliminary rulings before the ECJ on the validity of the Data Retention Directive. The national courts contested the compatibility of the Directive with Articles 7, 8 and 11 of the Charter of Fundamental Rights.[46] In *Tele2 Sverige,* a Swedish administrative Court and a UK Court of Appeal referred preliminary questions to the ECJ on the compatibility of respectively the Swedish laws on data retention[47] and the UK DRPIA[48] with the e-privacy Directive as well as with Articles 7 and 8 of the Charter of Fundamental Rights.[49]

---

[43] See European Commission's answer to the European Parliament on the PNR proposal and the consequences of the DRI judgment, as leaked by Statewatch, see <statewatch.org/news/2015/mar/eu-com-eu-pnr-letter.pdf> accessed 1 August 2017. The European Commission referred to 'legislation' in general, but one understands that its reasoning focuses on EU legislation and not on national legislation.

[44] ibid.

[45] Covering both domestic and cross-border data processing.

[46] *Digital Rights Ireland* (n 14) para 23; the national Courts asked the ECJ to review the compatibility of the Data Retention Directive with other EU provisions (art 41 Charter, art 52 (3)-(4)-(7) Charter, and art 8 ECHR); at national level, proceedings against national measures implementing the Data Retention Directive were brought by the advocacy group Digital Rights Ireland in Ireland and by more than 11,000 applicants and the regional Government of Carinthia in Austria.

[47] *Tele2 Sverige* (n 15) paras 15 and 16, respectively the Law 2003:389 on electronic communications (*Lagen (2003:389) om elektronisk kommunikation* or LEK) and Regulation 2003:396 on electronic communications (*Förordningen (2003 :396) om elektronisk kommunikation*); the Code of Judicial Procedure (*Rättegångsbalken* or RB) and Law 2012 :278 on the collection of data on electronic communications in the law enforcement authorities' investigative activities (*Lagen (2012 :278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*).

### *a. Elements of the Benchmark*

In both cases, the ECJ had to assess whether the data retention regimes at EU or national level constituted an interference with the right to privacy (Article 7 of the Charter) and with the right to data protection (Article 8 of the Charter) and if so, whether this interference was justified in application of Article 52(1) of the Charter.

*i) Existence of interferences?*

In each case, the Court did not find one but several interferences. First, the obligation to retain data and give law enforcement authorities access to them constitute two distinct interferences with the right to privacy.[50] Then, without although much explanation, the ECJ ruled in *Digital Rights Ireland* that the Data Retention Directive also constituted an interference with the right to data protection on the ground that 'it provides for the processing of personal data.' The Court clearly missed the opportunity to explain the nature and characteristics of metadata and the reasons why metadata should be considered personal data.[51] In *Tele2 Sverige*, the Court put more emphasis on the distinction between the interference based on the retention of data and the interference based on access to those retained data by law enforcement authorities.

*ii) Justifications*

After having established the existence of interferences, the Court assessed whether they were justified in application of Article 52(1) of the Charter. Article 52(1) sets the conditions under which fundamental rights, such as the rights to privacy and data protection, can be limited. First, limitations must be 'provided by law'. Second, they must 'respect the essence of those rights.' Third, they must comply with the principle of proportionality, meaning they must '[be] necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.'[52] The assessment of the Court in the two cases is different: in *Digital Rights Ireland*,[53] the Court analysed in detail the different conditions under which derogations to

---

[48] Opinion AG Saugmandsgaard ØE, *Tele2 Sverige*, paras 34 and 35, the data retention regime governed by the Data Retention and Investigatory Powers Act 2014 (DRIPA), the Data Retention Regulations 2014 (SI 2014/2042) and the Retention of Communications Data Code of Practice and the rules on access to communications data as defined in the Regulatory Investigatory Act 2000 as amendment by the Regulation of Investigatory Powers Order 2015 and the Acquisition and Disclosure of Communications Data Code of Practice, ECLI:EU:C:2016:572.

[49] At national level, proceedings were brought by *Tele2 Sverige*, a Swedish telecommunications provider that stopped retaining traffic data the day after the DRI judgment was delivered, and by three individuals who challenged the new UK data retention regime adopted after the invalidation of the DRI judgment; for more details, see para 48 et seq, and para 55 et seq.

[50] *Digital Rights Ireland* (n 14) para 32 et seq, and *Tele2 Sverige* (n 15) para 100.

[51] It is quite relevant to wonder which type of info metadata can reveal about an individual, see for instance, Jonathan Mayer, Patrick Mutchler, and John C. Mitchell, 'Evaluating the Privacy Properties of Telephone Metadata' (2013) 113 (20) Proceedings of the National Academy of Sciences of the United States of America, 5536; see also the position of the A29WP that considers metadata as personal data in A29WP, 'Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes' [2014] WP 215, where it states, page 4, that: 'unlike in other countries, in Europe, metadata are personal data and should be protected.'

[52] art 52(1) of the Charter of Fundamental Rights.

[53] *Digital Rights Ireland* (n 14) para 39 et seq; the Court assessed whether the Data Retention Directive infringed the essence of the rights to privacy and data protection (it did not) and checked whether the

the fundamental rights are permitted, whereas in *Tele2 Sverige*, the Court mainly focused on the proportionality of the national laws derogating to the principle of confidentiality.[54] Yet it is precisely on the last condition of Article 52(1) of the Charter, i.e. the test of proportionality, that both the Data Retention Directive and the national measures failed. The Court found that the Data Retention Directive and the national measures under review were not proportionate since they went beyond what was strictly necessary.

In *Digital Rights Ireland*, the Court held that the Directive did not 'lay down clear and precise rules governing the scope and application of the measure and imposing minimum safeguards' for the persons affected by the measures of data retention.[55] More specifically, concerning the law enforcement access to retained data, the Data Retention Directive did not provide any limits.[56] The Court found that the Directive failed to define an 'objective criterion' to limit law enforcement access[57] and also failed to provide "substantive and procedural conditions" on access and further use of the retained data by law enforcement authorities. In particular, the Court found that the Directive did not identify who could have access to the retained data and did not set a procedural rule imposing a prior independent review of the request for access.[58]



In *Tele2 Sverige*, the ECJ confirmed the conditions identified in *Digital Rights Ireland*. Concerning the objective of the national instruments, the Court held that national laws must determine the conditions of access to ensure that access is limited to what is strictly necessary but at the same time, national legislation must adopt 'substantive and procedural conditions governing the access' to the retained data by law enforcement authorities.[59] On that matter, the Court reiterated the conditions set out in *Digital Rights Ireland* in relation to the Data Retention Directive. Those include the (number of) persons entitled to get access to the retained data as well as a judicial or administrative prior review of the request for access.[60] In *Tele2 Sverige*, building on the case law of the European Court of Human Rights,[61] the ECJ specified that 'access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning or having committed a serious crime or of being implicated in one way or another in such a crime.'[62] Thus, a link with a serious criminal activity is necessary. In the *Tele2 Sverige* case, the Court added an extra safeguard to allow individuals to exercise their right of remedy: the Court imposed a duty of notification on law

objective of the data retention directive constituted an objective of general interest (it did as it aimed at fighting serious crime).
[54] *Tele 2 Sverige* (n 15) para 95 et seq.
[55] *Digital Rights Ireland* (n 14) para 54.
[56] *Digital Right Ireland* (n 14) para 60.
[57] *Digital Rights Ireland* (n 14) para 61: 'must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto.'
[58] *Digital Rights Ireland* (n 14) para 62.
[59] *Tele2 Sverige* (n 15) para 118.
[60] *Digital Rights Ireland* (n 14) para 62; *Tele2 Sverige* (n 15) para 118.
[61] In particular, *Roman Zakharov v Russia*, App no 47143/06 (ECHR, 04 December 2015).
[62] *Tele2 Sverige* (n 15) para 119.

enforcement authorities that have accessed the retained data. They have the obligation to inform individuals, according to their national laws, that their data have been accessed, as soon as this notification can no longer prejudice the investigations.[63] The Court thus considered that this obligation of information has to be implemented in national procedural laws.

In conclusion, on the issue of access to retained data, the Court set out 'procedural and substantive conditions' to frame that access. Laid down in *Digital Rights Ireland* and confirmed in *Tele2 Sverige*, EU or national measures relating to the collection of personal data and their further processing for law enforcement purposes should contain: an objective criterion to define how and when law enforcement authorities should be granted access to the data; a procedural rule on an independent prior review of the request for access, and the obligation to notify individuals whose personal data have been accessed. The next sub-section applies the findings of *Digital Rights Ireland* and *Tele2 Sverige* to determine whether Directive 2016/680 contains the conditions necessary to govern law enforcement access to personal data collected by private parties for a non-law enforcement purpose.

### 3. Application of the Rulings to Directive 2016/680

Preliminarily, it should be observed that *Digital Rights Ireland* was decided while Directive 2016/680 was being negotiated. Therefore, and for the reasons explained in the previous sub-section, its findings should have been taken into account and 'implemented' in Directive 2016/680. One should expect to find in the Directive the conditions identified in *Digital Rights Ireland,* i.e. the number of persons allowed to access the personal data as well as a procedure of prior review of the request for law enforcement access. By contrast, *Tele2 Sverige* was decided after the adoption of Directive 2016/680. It is therefore logical that its findings, and in particular, the obligation of notification, might not be found in Directive 2016/680.

This section suggests a reading of the safeguards established in *Digital Rights Ireland* and *Tele2 Sverige* in the broader context of law enforcement access to personal data held by private parties. If the safeguards have not been established for that specific scenario, they can still apply since the findings of the judgments reach beyond data retention measures.[64]

#### *a. Objective Criteria to Determine Law Enforcement Access*

First, the objective of Directive 2016/680 is to lay down data protection rules when personal data are processed by law enforcement authorities for 'the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against the prevention and the prevention of threats

[63] *Tele2 Sverige* (n 15) para 121.
[64] See sub-section 1 ('Preliminary Remarks on the Use of Digital Rights Ireland and Tele2 Sverige as Benchmark') of Section III.

to public security.'[65] This objective is a general objective of fighting crime. As such it constitutes an objective of general interest.[66] However, the objective of fighting crime is not enough to grant access to law enforcement authorities. In *Digital Rights Ireland* and *Tele2 Sverige*, the Court considered that the objective should at least be an objective of fighting serious crime.[67] Access to retained data needs to be justified by the nature of the crime. However, in the scenario under review, personal data are not retained for future access by law enforcement authorities; they are only made available if requested. As such, in a criminal investigation context, it seems difficult to argue that law enforcement authorities should only get access to personal data relating to serious crime. Though, in the context of criminal intelligence where indices that a criminal activity has occurred or will occur are not established yet, it would make sense to limit the access to personal data that are linked to serious crime, so as to prevent the mass surveillance of individuals. Thus, concerning the objective criterion of the conditions of access, a distinction between criminal investigation and criminal intelligence is necessary in relation to the nature of the criminal activity at stake. Yet Directive 2016/680 does not establish such a distinction.

Moreover, what is missing from Directive 2016/680 is the identification of individuals authorised to have access to the personal data collected for a different purpose (staff of law enforcement authorities) and the categories of personal data that should be accessible (personal data from suspects, criminals, witnesses, etc.). On this issue, the leaked version of the draft 'police' Directive of 2011 contained a specific provision. Article 4(2)(a) proposed restraining the access to cases where 'reasonable grounds give reason to consider that the processing of the personal data will substantially contribute to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.'[68]



#### *b. Oversight Mechanism: Independent Review of the Request for Access?*

In *Digital Rights Ireland*, the ECJ ruled that law enforcement access to retained data should be subject to a prior review, either by a Court or by an independent administrative body. The procedure should be part of national criminal procedural law.[69] The ECJ leaves some leeway to Member States in the implementation of the review mechanism. The question is whether Directive 2016/680 contains a procedural safeguard that ensures prior review of the request for access to personal data.

[65] art 1(1) of Directive 2016/680.
[66] *Digital Ireland Rights* (n 14) para 41 et seq.
[67] *Digital Ireland Rights* (n 14) paras 42-43, and *Tele2 Sverige* (n 15) para 102.
[68] art 4(2)(a) of the leaked draft version of the proposal for a 'police Directive' (n 17).
[69] *Digital Rights Ireland* (n 14) para 62, as complemented by *Tele2 Sverige* (n 15) para 120. The prior review is initiated 'following a reasoned request of those authorities submitted within the procedures for the prevention, detection or prosecution of crime.'

Article 28 of Directive 2016/680 provides for an oversight mechanism. It requires the 'prior consultation' of the national data protection authority (DPA) in two cases:[70] when a data protection impact assessment has been performed and no risk-mitigating measure has been adopted (Article 28(1)(a)) or when a specific processing 'involves a high risk to the rights and freedoms of individuals' (Article 28(1)(b)).[71] It could be argued, with a far-stretched interpretation of Article 28(1)(b), that law enforcement access to personal data collected by private parties for a non-law enforcement purpose falls within the category of 'high-risk processing'. However, not all access to personal data for a law enforcement purpose would qualify as 'high risk processing'. If the notion is undefined,[72] Recital 52 of Directive 2016/680 provides some guidance to assess the level of risk of a processing. The purpose of the processing is one of the factors, besides the nature, scope, and context of the processing. Determining whether a subsequent processing of personal data for a law enforcement purpose constitutes a 'high risk' processing requires a case-by-case analysis. Therefore, it could be that the further processing of personal data would constitute a 'high risk' processing in a context of criminal intelligence because of the risk of mass surveillance; whereas the same processing performed in a criminal investigation context would not.

In the end, it is still questionable whether the procedure of 'prior consultation' of a national DPA set out in Article 28 of Directive 2016/680 amounts to the procedure of 'prior review' by an independent authority, as required by the ECJ case law. If DPAs are independent authorities,[73] it cannot be claimed that a 'prior consultation' is equivalent to a 'prior review'. Directive 2016/680 indeed lacks clarity on the exact power given to data protection authorities through the prior consultation. Article 47(3) of Directive 2016/680, on the powers of national supervisory authorities, refers to their 'advisory power' in respect of the procedure of prior consultation. Likewise, if it is justified to require a prior judicial or administrative review of a request for access to personal data collected for a different purpose, it might be disproportionate to require the review of each request by a national DPA.

In conclusion, Article 28 of Directive 2016/680 does not seem to be a sufficient procedural safeguard. First of all, it is not guaranteed that all data protection authorities across the EU would have the same reading of Article 28 of Directive 2016/680. Then, the provision only

[70] Besides the two cases requiring prior consultation of the DPA, Member States have the possibility to establish a list of processing operations that are subject to prior consultation. One could imagine that the case of law enforcement access to personal data generated by third parties could be included in such a list; however this option is left to the discretion of Member States, see art 28(3) Directive 2016/680.
[71] art 28(1)(b) Directive 2016/680.
[72] Recital 52 Directive 2016/680 only specifies that high risk is 'a particular risk of prejudice to the rights and freedoms of data subjects'; by comparison in the context of the GDPR, art 35(3) of the Regulation provides some guidance on what 'high risk processing' might include: systematic profiling, large-scale processing of sensitive data or systematic and large-scale monitoring of publicly accessible areas.
[73] Following both the GDPR and Directive 2016/680, DPAs are required to be independent authorities; on their independence, see among others, Orla Lynskey, 'the *Europeanisation* of Data Protection Law' (2017) 19 Cambridge Yearbook of European Legal Studies 252.

requires an advice (prior consultation) and not a decision (prior review) before the further processing for a law enforcement purpose can be executed. Finally, the prior consultation of DPAs is limited to 'high risk processing'.

#### *c. The Right to Information as a Duty of Notification?*

The right to be informed about the collection of one's own personal data is a very important right since it triggers the application of the other data subjects' rights: the right to access the personal data collected; to rectify them if they are inaccurate; to have them erased under specific conditions, as well as to be informed of the right of legal remedies. In a law enforcement context, it is logical that those rights are not as broad as in a non-law enforcement context. For instance, the necessity of a criminal investigation may validly justify restrictions to those rights. However, following *Tele2 Sverige,* individuals whose personal data have been accessed by law enforcement authorities should be notified as soon as possible and, in any event, as soon as the notification no longer prejudices the ongoing investigations.[74]

Article 13 of Directive 2016/680 sets out the right of information, which is defined as 'information to be made available or to be given to the data subject.' This provision lists all the pieces of information to be 'made available or given' to an individual. However, it does not specify that the information be actively provided to the data subject. The wording of Article 13 seems to indicate that the right to information is a right of confirmation that collection of personal data has been carried out. The right to information, as set out in Article 13 of Directive 2016/680, constitutes an improvement in comparison with Article 16 of the Council Framework Decision 2008/977/JHA. This latter only provides for a right 'to be informed' in accordance with 'national law.' Yet, Article 13 of Directive 2016/680 does not establish a duty of notification. Nowhere is it mentioned in the Directive that data subjects should receive communication about the collection of their data as soon as the purpose for which their data have been collected is not at stake anymore. By comparison principle 2.2 of the Council of Europe's Recommendation on the use of personal data in the police sector (Recommendation R(87)15) provides that the individual should be 'informed that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.'[75]

The absence of notification is even more problematic in a case where personal data have been collected by private parties under the GDPR regime and are accessed for further use by law enforcement authorities. The individuals concerned are not able to exercise their rights properly if they are not informed, at some point, that their data have been accessed. In *Tele2 Sverige*, the ECJ required that law enforcement authorities 'notify the persons

[74] *Tele2 Sverige* (n 15) para 121.
[75] However, law enforcement authorities have criticised this principle because they consider it difficult to put into practice.

affected, under the applicable national procedures.'[76] The Court added that the notification is 'necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy.'[77] However one could dispute the legal basis on which the ECJ imposes a duty of notification on law enforcement authorities for the further processing of the retained data. The Court based its reasoning on Article 15(2) of the e-privacy Directive 'read together' with Article 22 of the Data Protection Directive.[78] Yet the Data Protection Directive does not apply to the processing of data for law enforcement purposes. Those processing operations are excluded from the scope of EU law except when they are exchanged between Member States. Cross-border data processing for law enforcement purposes falls within the scope of Council Framework Decision 2008/977/JHA.[79] But, thanks to a clever artifice, the ECJ held that both the retention of data by telecoms operators and their access by law enforcement authorities fell within the scope of the e-privacy Directive. To reinforce its position, the Court added that the only reason that the data were retained was to provide law enforcement authorities access to them.[80] As mentioned in sub-section 2, the reasoning of the ECJ on this specific issue is disputable. With the adoption of the new data protection framework, the scenario of access by law enforcement authorities to retained personal data should be considered as a processing for a law enforcement purpose and fall within the scope of Directive 2016/680.[81] However, beyond the possible discussion on the scope of the e-privacy Directive and the inclusion of law enforcement access, one should focus on the interpretation of the right to information given by the ECJ. In a scenario of law enforcement access to personal data generated in a different context, the right to information ought to be interpreted as a duty of notification. Yet as drafted, Article 13 of Directive 2016/680 does not lay down such an obligation.

After the analysis of the ECJ case law on data retention and its possible impact on the safeguards contained in the 'police' Directive, the article will assess whether the principle of purpose limitation, as defined in Directive 2016/680, plays its role of safeguard in the context of law enforcement access.

## IV. Safeguards against Abuses: The Principle of Purpose Limitation?

In the scenario at stake as well as in the scenario of data retention of personal data, the main issue from a data protection perspective is the change of initial purpose: personal data collected for a specific purpose are then reprocessed for a different purpose. As stated by the A29WP in its opinion on purpose limitation (Opinion 03/2013), the principle

[76] *Tele2 Sverige* (n 15) para 121.
[77] ibid.
[78] ibid.
[79] Recital 6 Council Framework Decision 2008/977/JHA.
[80] *Tele2 Sverige* (n 15) para 79.
[81] See Recital 19 GDPR making a bridge between the GDPR and the Directive in case of further use by law enforcement authorities of personal data collected under the GDPR.

of purpose limitation is 'a cornerstone of data protection.'[82] It constitutes a safeguard against the misuse or abuse of personal data and guides the lawful use of personal data collected for a different purpose.

In a situation where law enforcement authorities get access to personal data generated by private parties, the purpose of the further processing of personal data (law enforcement purpose) has no link with the initial purpose of data collection (commercial or operational purpose). As such, the purpose of the further processing should be deemed incompatible with the initial purpose of processing. Yet, Article 4(2) of Directive 2016/680 allows the repurposing of personal data collected by other parties for a different purpose under the conditions of legality and proportionality. The question that arises is whether this provision offers sufficient guarantees to protect individuals whose personal data are collected under the regime of the GDPR and subsequently used under the regime of the 'police' Directive.

### 1. Notion of Purpose Limitation

Described in identical terms in the GDPR and the 'police' Directive, the principle of purpose limitation entails that personal data are 'collected for specified, explicit, and legitimate purposes and not processed in a manner that is incompatible with those purposes.'[83] This wording originates from Article 6(1)(b) of the Data Protection Directive. As analysed by the A29WP, the principle of purpose limitation is composed of a principle of purpose specification ('specified, explicit and legitimate purposes') and a principle of compatible use ('not processed in a manner incompatible').[84] Since the focus of this paper is on the further processing of personal data and not on their initial processing, it is assumed that the purpose of initial processing satisfies the criteria of purpose specification. For the same reason, the terms 'purpose limitation' and 'principle of compatible use' are used interchangeably in this section.



### 2. Application of the Principle: Test of Compatibility versus Derogation

The interpretation given to the principle of purpose limitation is different in a non-law enforcement context from that in a law enforcement context. When the GDPR applies, the compatibility of a further processing with the initial processing is assessed in application of a test of compatibility based on five factors as described in Article 6(4) GDPR. Those include the link between the initial processing and the further processing; the context of data collection; the nature of personal data (such as sensitive data); the impact of the further processing on data subjects, and the existence of appropriate safeguards to compensate for the change of purpose(s).[85] The factor of "context of processing" should, in

[82] A29WP, 'Opinion 03/2013 on purpose limitation' [2013] WP 203, 4.
[83] art 5(1)(b) GDPR and art 4(1)(b) of Directive 2016/680.
[84] Opinion 03/2013 (n 82).
[85] art 6(4) GDPR reads as follows: 'Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose

particular, be understood as "reasonable expectations of data subjects based on their relationship with the controller as to their further use."[86] These factors apply if the further processing is not based on the data subject's consent for the further processing or on national or EU law allowing the further processing.[87]

By contrast, in a law enforcement context, the compatibility of a further processing is not assessed in application of a test of compatibility. Instead, Article 4(2) of Directive 2016/680 provides for a derogation from the principle of purpose limitation: the further processing of personal data for a purpose different than the initial purpose of collection is allowed if it complies with the principles of legality (i.e. based on "Union or Member State law") and proportionality ("processing necessary and proportionate to that other purpose").[88]

Article 4(2) of Directive 2016/680 raises at least two issues: the first one relates to the initial processing of personal data and the second one to the compatibility of the further processing of personal data for a law enforcement purpose with the initial purpose of their collection in a non-law enforcement context.

First, from the wording of Article 4(2) of Directive 2016/680, it is not clear which type of 'initial purpose' is referred to. The first sentence of Article 4(2) provides that "the processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted…" Should the phrase "other than that for which" be understood as referring to any purpose other than those of Directive 2016/680, i.e. any non-law enforcement purpose? Alternatively, should it be understood as referring to any initial purpose covered by Directive 2016/680 but different from the purpose of further use? In that case, the initial and further purposes are of the same nature, i.e. they fall within the broad category of law enforcement, but they are different. For instance, one could think of personal data collected in the context of a specific criminal investigation and further used in a non-related investigation. In the end,

is compatible with the purpose for which the personal are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.'

[86] Recital 50 GDPR.

[87] art 6(4) GDPR.

[88] art 4(2) Directive 2016/680 reads as follows: 'Processing by the same or another controller for any of the purposes set out in Article 1(1) other than for which the personal data are collected shall be permitted in so far as: (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.' Art 4(2) GDPR needs to be read together with Recital 29 Directive 2016/680.

the wording of Article 4(2) of Directive 2016/680 remains ambiguous[89] and allows for a broad interpretation that encompasses any initial purpose of processing within or outside the scope of Directive 2016/680.

Next, in application of Article 4(2) of Directive 2016/680, the further processing is authorised provided it is based on a national or EU law, and it is necessary and proportionate to the purpose of law enforcement. Yet, that article establishes no link between the purpose of the initial processing and the purpose of the further processing. Does it mean that the further purpose is incompatible per se with the initial purpose of processing? It is at least not possible to draw that conclusion from the wording of Directive 2016/680. As a matter of comparison, under the GDPR, unrelated purposes of processing are not considered incompatible per se. For instance, Article 5(1)(b) of the GDPR clearly establishes that the further processing for a scientific, historical or statistical purpose is not incompatible with the initial purpose of processing, as long as it is accompanied with appropriate safeguards.[90] However, in a law enforcement context, Directive 2016/680 does not contain a similar provision. Article 4(2) of Directive 2016/680 does not even refer to the notion of compatibility between the initial and the further purposes of processing. Instead, it authorises the subsequent processing under specific conditions. The provision seems to establish a derogation from the principle of 'purpose limitation' described in Article 4(1)(b) of Directive 2016/680. Yet, the approach followed in Directive 2016/680 is different from the one that the A29WP advocated in Opinion 03/2013. In that Opinion, the A29WP reviewed several mixed scenarios involving an initial collection of personal data for a non-law enforcement purpose followed by a re-use of those data for a law enforcement purpose. These specific scenarios relate to the Data Retention Directive, the PNR scheme, the EURODAC database and the use of smart metering data for the purpose of detecting tax fraud.[91] In the analysis of the different examples, the A29WP did not state that the further processing was prima facie incompatible with the original purpose of processing. Instead, it performed a test of compatibility, weighing the further processing for a law enforcement purpose against the initial purpose of collection using various factors. The A29WP based its whole reasoning on the initial purpose of collection. If that purpose fell within the scope of the Data Protection Directive, the further processing –whatever its nature- had to be assessed following the test of compatibility the A29WP had defined.

What is problematic in the approach of the principle of purpose limitation set out in Directive 2016/680 is the absence of test of compatibility, which is replaced instead by a derogation based on the principles of necessity and proportionality. Yet, as rightly observed by the European Data Protection Supervisor in respect of the further use for a

[89] Recital 29 Directive 2016/680 does not bring further clarification as it relates to 'personal data [that] are processed by the same or another controller for a purpose within the scope of this Directive other than that for which it had been collected…'
[90] Appropriate safeguards as defined in art 89(1) GDPR.
[91] Opinion 03/2013 (n 82) Annex 4, examples 17 to 20, 67-69.

law enforcement purpose of large-scale databases initially constituted for administrative purposes: 'a database regarded as proportionate when used for a specific purpose can become disproportionate when the use is expanded to other purposes afterwards.'[92] To acknowledge this situation, some authors have even redefined the principle of purpose limitation as a principle of 'purpose deviation' that reflects the absence of links between the initial and the further purposes of processing.[93] It is therefore the role of the ECJ to interpret the principles of necessity and proportionality in a way that will ensure the protection of data subjects. To do so, the Court ought to take into account the initial purpose of processing in its interpretation of the principle of proportionality as provided under Article 4(2) of Directive 2016/680.

## V. Conclusions

The scenario of law enforcement access to personal data initially collected for a different purpose raises complex issues. If it is established that the further processing of those data for a law enforcement purpose falls within the scope of Directive 2016/680, no specific rules taking into account that scenario have been adopted. However, in light of two ECJ's rulings, *Digital Rights Ireland* and *Tele2 Sverige,* on partially similar scenarios, the assessment of the rules contained in Directive 2016/680 reveals that the Directive lacks essential provisions to ensure the protection of individuals' right to data protection. In particular, the Directive fails to provide objective criteria to delimit the law enforcement access to personal data generated for a different purpose and a specific procedural rule on the prior review of the request for access. As for the right to be informed, it should be interpreted, in that context, as a right to be notified, at a certain point, that data have been accessed by law enforcement authorities. The article also points out that the absence of specific rules is also detrimental to the principle of purpose limitation, which does not link the initial purpose of processing with the purpose of further processing.

To overcome these shortcomings, several solutions could be envisaged. First, since the Directive has recently been adopted, a revision of the Directive to incorporate rules specific to the scenario is simply not a practical option.

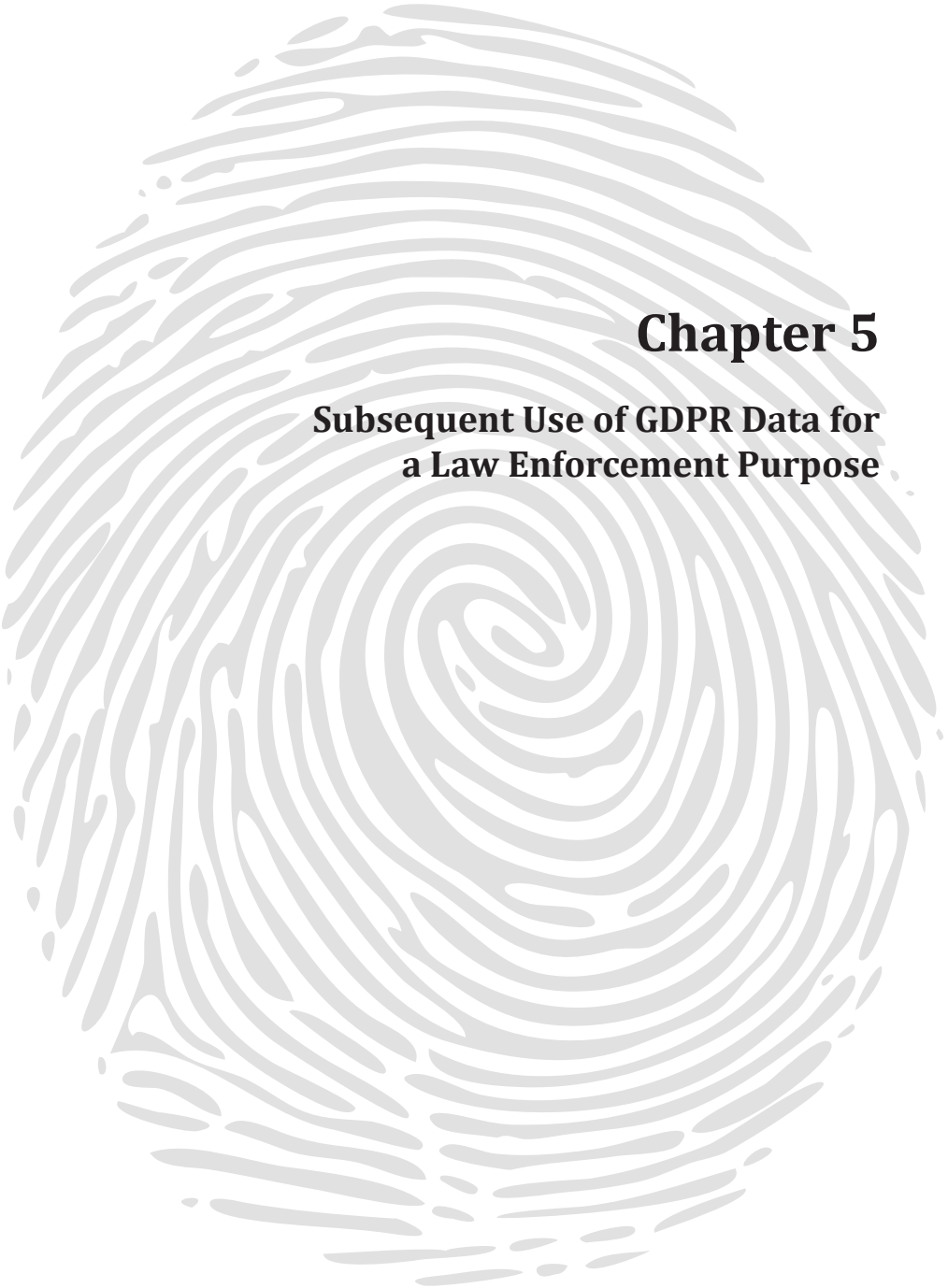
As a solution, one could consider the opportunity provided by the ongoing revision of the e-privacy Directive to add specific rules, based on the findings of *Digital Rights Ireland* and *Tele2 Sverige*, to cover the scenario of law enforcement access to personal data generated

[92] See EDPS, 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration' [2012] OJ C34/18, para 17; EDPS, 'Opinion 07/2016, EDPS Opinion on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations) [2016], para 17 <https://edps.europa.eu/sites/edp/files/publication/16-09-21_ceas_opinion_en.pdf> accessed 1 August 2017.
[93] e.g. Els de Busser and Gert Vermeulen, 'Towards a Coherent EU Policy on Outgoing Data Transfers for Use in Criminal Matters? The Adequacy Requirement and the Framework Decision on Data Protection in Criminal Matters. A Transatlantic Exercise in Adequacy' in Marc Cools et al (eds), *EU and International Crime Control. Topical Issues,* Governance and Security Research Paper Series, Vol.4 (Maklu 2010) 102.

by private parties. This option would, however, be limited to the further use of personal data originally processed by telecommunications providers only. Therefore, this option would be quite restrictive.

The second option would be in the hands of the European Data Protection Board, which could issue an opinion on the data protection rules applicable to the scenario, including the implications of *Tele2 Sverige* on the interpretation of Directive 2016/680. The main drawback of this option lies in its non-binding nature.

Ultimately, and this last option would offer more legal certainty, after the implementation of Directive 2016/680 in national legislation, national courts could send preliminary questions to the ECJ on the interpretation of the key provisions of Directive 2016/680 (and in particular on the right to be informed, the procedure of prior review by DPAs and on the derogation to the principle of purpose limitation). This option might not be fast. And one might need, in the end, the resilience and activism of another Schrems to start tailor-made proceedings at national level and pave the way to the ECJ.



# Chapter 5

## Subsequent Use of GDPR Data for a Law Enforcement Purpose

## *Chapter 5: Subsequent Use of GDPR Data for a Law Enforcement Purpose*

*The Forgotten Principle of Purpose Limitation?*[*]

**Abstract:**
*This article questions the role of the principle of purpose limitation in a situation where personal data are collected under the General Data Protection Regulation (GDPR) and further processed under the regime of the 'police and criminal justice' Directive. It reviews the rules set out in both instruments, concerning the principle of purpose limitation and the further processing of personal data for a different purpose. The analysis of the rules under Directive 2016/680 reveals some ambiguity: are the rules applicable to the subsequent use of any personal data (including those collected under the GDPR)? Or are the rules limited to the subsequent use of 'police or criminal justice' data? Building on the ambiguous wording of Article 4(2) of the Directive, the article addresses the two hypotheses and analyses their consequences. It concludes with the uncertainty of the applicable rules and the likelihood of diverging interpretations at the national level.*

### I. Introduction

Examples of cases where law enforcement authorities request access to personal data initially collected by third parties for a different purpose are numerous. Many of them relate to the legal obligation of private parties to retain and disclose personal data to law enforcement authorities, such as in the fields of air transport,[1] banking[2] or telecommunications.[3] In these cases, personal data are retained for further use by law enforcement authorities to fight fraud, terrorism, and serious criminal offences. Besides these cases, there are situations where private parties collect personal data for their own uses (such as commercial or operational purposes) but are under no specific obligation to retain them for law enforcement purposes. One could think of the vast amount of personal data that social media collect and hold. Some of these data are very valuable to law

[*] Article published in the European Data Protection Law Review (EDPL), volume 4, issue 2, June 2018, pages 157-162; the author wishes to thank Prof Jeanne Mifsud Bonnici for her valuable comments and Pim Geelhoed for fruitful discussions on law enforcement issues, as well as the peer-reviewers for their suggestions and careful reading. The views expressed in this article are solely those of the author. All remaining errors are the author's sole responsibility.

[1] Obligation imposed on airline companies to retain passenger data; see Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes (PNR Directive)[2016] OJ L119/32.

[2] Obligations imposed on banks to retain financial data for anti-money laundering purposes.

[3] Referring to the Data Retention Directive (Directive 2006/24/EC) adopted in 2006 and invalidated in 2014 by the European Court of Justice; see Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* and *Seitlinger and Others* [2014] ECLI:EU:C:2014:238.

enforcement authorities (i.e. photographs or voice recordings). Although social media are not obliged to retain these data, they can be requested to grant law enforcement authorities access to the data. As shown by the transparency reports published by the largest tech companies (e.g. Facebook, Google, Microsoft), the number of law enforcement requests for access to content and user accounts is rapidly growing.[4] No figure is, however, available on the types of content requested and the purposes of use. It is also almost impossible to know the exact volume of personal data collected and held by social media. Concerning photographs alone, in 2012, more than 300 million photos were uploaded to Facebook every day.[5] Yet, as shown by the research undergone by Facebook on the uploaded images, photographs portraying individuals are very useful for facial recognition.[6] In a different field, one could also think of biometric data (such as fingerprints, palm prints, and facial images) that an employer or a school holds about their employees or students to give them access to premises, canteens or library facilities. These data are particularly valuable for identification purposes. It is, thus, not hard to imagine that law enforcement authorities could ask private parties to hand over biometric data initially collected for a purpose other than law enforcement and re-use them in the context of a criminal investigation.[7]

Due to the availability of data and technological means to process them, the repurposing of data – in the sense of re-use for a different purpose – is a growing phenomenon.[8] When personal data are repurposed to be used in a different context, that repurposing might challenge the principle of purpose limitation. Following that principle, personal data collected for a specific purpose should be used for compatible purposes or further processed under a different legal basis. The situation becomes complicated when personal data have been collected in a particular context (such as commercial) and are further processed in a different one (such as law enforcement). But when rules on data protection are split between two instruments, like in the new EU data protection framework, the



[4] See Aliya Ram, 'Tech Companies Endure Near-Doubling of Requests for Personal Data' *Financial Times* (30 August 2017) <https://www.ft.com/content/b754882e-8cbd-11e7-9084-d0c17942ba93> accessed 10 April 2018.
More specifically Facebook's Transparency Report <https://newsroom.fb.com/news/2017/12/reinforcing-our-commitment-to-transparency/> accessed 10 April 2018.
Microsoft's Transparency Report < https://www.microsoft.com/en-us/about/corporate-responsibility/lerr > accessed 10 April 2018.
Google's Transparency Report <https://transparencyreport.google.com/user-data/overview> accessed 10 April 2018.
[5] Casey Chan, 'What Facebook Deals with Everyday: 2.7 Billion Likes, 300 Million Photos Uploaded and 500 Terabytes of Data' *Gizmodo* (22 August 2012) <https://gizmodo.com/5937143/what-facebook-deals-with-everyday-27-billion-likes-300-million-photos-uploaded-and-500-terabytes-of-data > accessed 10 April 2018.
[6] Joaquin Quiñonero Candela, 'Managing Your Identity on Facebook with Face Recognition Technology' *Facebook Newsroom* (19 December 2017) <https://newsroom.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/> accessed 10 April 2018.
[7] On the collection of biometric data by schools and their potential re-use by law enforcement authorities, see for instance Wendy Grossman, 'Is School Fingerprinting out of Bounds?' *The Guardian* (30 March 2006) <https://www.theguardian.com/technology/2006/mar/30/schools.guardianweeklytechnologysection> accessed 10 April 2018.
[8] Especially with big data analytics, see Bart Custers and Helena Ursic, 'Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection' (2016) 6(1) International Data Privacy Law 4.

situation becomes even more complicated. The new framework is composed of a general instrument – the General Data Protection Regulation (GDPR)[9] – and of a specific instrument applicable to data processing in the field of law enforcement –Directive 2016/680 (Police and Criminal Justice Directive).[10] The GDPR replaces Directive 95/46/EC (Data Protection Directive),[11] while Directive 2016/680 replaces the Council Framework Decision 2008/977/JHA.[12] How do the instruments interact with each other when personal data collected under the GDPR are further processed under the rules of the new Directive? And what is the role of the principle of purpose limitation in such a scenario?

By investigating the rules applicable to the further processing of GDPR data in a law enforcement context, the article attempts to delineate the scope and role of the principle of purpose limitation when data processing is carried out across the two instruments. The paper only covers the subsequent use of GDPR data by law enforcement authorities under the new Directive. It does not tackle the issue of disclosure (which can entail the transfer) of personal data by private parties to law enforcement authorities.[13] According to Recital 11 of Directive 2016/680, this disclosure should be covered by the rules of the GDPR.[14] Following Purtova's analysis, the disclosure of personal data by private parties to law enforcement authorities is subject to the GDPR and might benefit from the exceptions of Article 23 GDPR.[15] This article analyses, instead, the rules applicable to the re-use of GDPR data once the data have been accessed by or transferred to law enforcement authorities.

Following this introduction, Section II sketches the background on the principle of purpose limitation and addresses the relationship between the GDPR and Directive

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
[10] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing the Council Framework Decision 2008/977/JHA [2016] OJ L119/89.
[11] European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC or Data Protection Directive) [1995] OJ L281/31.
[12] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Council Framework Decision 2008/977/JHA) [2008] OJ L 350/60; the new Directive extends the scope of the Council Framework Decision limited to cross-border processing.
[13] Nadezhda Purtova, 'Between the GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships' (2018) 8(1) International Data Privacy Law 52.
[14] Recital 11 GDPR provides that 'Regulation (EU) 2016/679, therefore, applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject'; for a criticism on the meaning and scope of Recital 11, see Mireille Caruana, 'The Reform of the EU Data Protection Framework in the Context of Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement' (2017) International Law Review, Computers & Technology (online)
<http://www.tandfonline.com/doi/abs/10.1080/13600869.2017.1370224 > accessed 10 April 2018.
[15] It should be observed that art 23 GDPR sets out exceptions applicable to data subjects' rights and the corresponding data protection principles; one could question whether any data subject's right derives from the principle of purpose limitation, and thus whether art 23 GDPR could be invoked.

2016/680. Against this background, Section III compares the regime of the principle of purpose limitation in both instruments. It focuses on Article 4(2) of Directive 2016/680 providing the conditions applicable to further processing and questions the scope of the initial processing. Highlighting the textual ambiguity of Article 4(2), Section IV suggests a reading of the provision to encompass further processing of GDPR data, whereas Section V assesses the consequences of excluding such processing from the scope of Article 4(2).

## II. Background

This section briefly describes the roots of the principle of purpose limitation and addresses the relationship between the GDPR and Directive 2016/680.

### 1. Origin of the Principle of Purpose Limitation

The roots of the principle are to be found in early international instruments on privacy, and in particular in the OECD guidelines on privacy[16] and in the Council of Europe's Convention on the processing of personal data (Convention 108).[17] From the origin, the principle was split into two principles, a *purpose specification* principle and a *use limitation* principle.[18]In the law enforcement sector, the Council of Europe's Recommendation on the use of personal data in the police sector [Recommendation R(87) 15] also contains a provision on purpose limitation.[19]

Building on Convention 108, both the Data Protection Directive (Directive 95/46/EC) and the Council Framework Decision (Decision 2008/977/JHA) contain specific provisions on purpose limitation, although phrased slightly differently.[20] In both texts, the principle of purpose limitation entails that the purposes of data collection are 'specified, explicit and legitimate' and that data should not be further processed in a way 'incompatible with' the original purposes of collection.[21]

As acknowledged by the European Commission in its study on the implementation of the Data Protection Directive, the broad wording of the principle of purpose limitation has led to diverging interpretations in Member States. These differences concern the scope of

[16] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [1981] (updated in 2013) ('OECD Guidelines on Privacy')
<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm > accessed 10 April 2018.
[17] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS, No 108, 28 January 1981, Strasbourg (Convention 108).
[18] Respectively para 9 (purpose specification principle) and para 10 (use limitation principle) of the OECD Guidelines on Privacy.
[19] Council of Europe Recommendation R (87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector [1987], Principle 2.1 (purpose limitation) to be read together with Principle 4 (use limitation).
[20] art 6(1)(b) Directive 95/46 and art 3 Council Framework Decision 2008/977/JHA; art 3(1) of the Decision provides that: 'personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected.' The condition 'same purpose' is not to be found in Directive 95/46/EC.
[21] art 6(1)(b) Directive 95/46/EC and art 3(2) Council Framework Decision 2008/977/JHA.

exceptions, the meaning of compatible uses, and the requirement (as well as the type) of safeguards applicable to data subjects.[22]

The rationale of the principle in a law enforcement context is not to be found in Directive 2016/680. Instead, it is described in the Europol Regulation (Regulation 2016/794) on law enforcement cooperation.[23] The principle of purpose limitation is defined by its characteristics, which are 'to contribute to transparency, legal certainty and predictability.'[24] According to some authors, the principle of purpose limitation is the result of the right to self-determination, i.e. to control how own personal data are processed and used.[25] However, this approach and understanding of the principle are hard to support in a law enforcement context. In the context of a criminal investigation, it is indeed difficult to argue that an individual whose personal data have been collected for a commercial purpose should control the way the police further use his or her data. Instead, it could be argued that an individual whose data are further processed for a law enforcement purpose should be made aware, or be notified, about this processing after the investigation is over or as soon as the investigation cannot be prejudiced anymore.[26] Awareness or notification is, however, different from control.

Last, the principle of purpose limitation – in particular, its specification component – is an element of the fundamental right to the protection of personal data.[27] The Court of Justice of the European Union (CJEU) has recently acknowledged that 'the protection against unlawful access and processing' is a part of the 'essence' of the fundamental right to data protection.[28] As such, any limitation to the principle of purpose limitation should comply with the conditions formulated in Article 52(1) of the Charter of Fundamental Rights (the Charter). This claim will be further explained in the article.

### 2. Relationship between the GDPR and Directive 2016/680

As argued elsewhere,[29] the GDPR and Directive 2016/680 build a bridge towards each other. Recital 19 GDPR delineates the material scope of the Regulation. It excludes from its

[22] Annex 2, Evaluation of the Implementation of the Data Protection Directive, at 25 in Commission Staff Working Paper, Impact Assessment Accompanying the proposals for a Regulation and Directive, SEC (2012) 72 final [2012].
[23] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for law enforcement cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (Europol Regulation) [2016] OJ L135/53.
[24] Recital 26 Europol Regulation.
[25] Liane Colonna, 'Data Mining and its Paradoxical Relationship to the Purpose of Limitation' in Serge Gutwirth, Ronald Leenes, and Paul de Hert (eds), *Reloading Data Protection* (Kluwer 2014), 300-302; Maria Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing 2017) 40.
[26] As discussed later in the article.
[27] art 8 Charter.
[28] *Opinion 1/15 of the Court (Grand Chamber) on the Draft Agreement between Canada and the European Union* [2017] ECLI:EU:C:2017:592, para 150; also as cited and analysed by Coudert in Fanny Coudert, 'The Europol Regulation and Purpose Limitation, From the 'Silo-Based Approach' to…What Exactly ?' (2017) 3(3) EDPL 313.
[29] eg Catherine Jasserand, 'Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?' (2018) 34(1) Computer Law & Security Review; see also analysis made by Purtova (n 13).

scope the processing of personal data by 'public authorities' for a law enforcement purpose, as defined in Article 1(1) of the Directive. Those processing operations fall instead within the scope of Directive 2016/680.[30] Likewise, Recital 11 of the Directive expressly excludes from its scope processing activities by entities or bodies entrusted for law enforcement purposes when those processing activities are not carried out for a law enforcement purpose but for a purpose that would fall under the GDPR.[31]

Besides the two recitals on the material scope of each instrument, the GDPR and Directive 2016/680 are pretty silent on their relationship. As adopted, the texts are far less ambitious than the European Parliament's resolutions on the legislative proposals.[32] More specifically, the resolution on the proposal for a new Directive included an article on law enforcement access to personal data initially collected for a non-law enforcement purpose.[33] In that case, not only did the further processing need a legal basis but it also had to comply with strict conditions (such as identification of individuals allowed to access the data, adoption of safeguards, and specific format for the request).[34] In addition, the provision limited the re-use of the data to the 'investigation' or 'prosecution of criminal offences.'[35] Subsequent use of personal data for crime prevention was, thus, not envisaged.

There is not much discussion concerning the applicability of the new Directive rules to the law enforcement use of personal data collected by private parties. If carried out by a competent authority,[36] for one of the purposes of Directive 2016/680,[37] the subsequent use of GDPR data falls within the scope of the Directive. What is more crucial is to determine the rules applicable to the further processing of GDPR data under the regime of Directive 2016/680. To address this issue, next section assesses the principle of purpose limitation as designed in Directive 2016/680.



[30] See art 2(2) GDPR and Recital 19 GDPR.
[31] See Recital 11 Directive 2016/680.
[32] Respectively European Parliament Legislative Resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011-C7-0025/2012-2012/0011(COD) P7_TA(2014)01[2014], and European Parliament legislative Resolution on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data [COM(2012)0010-C-7-0024/2012-2012/010(COD)] P7_TA(2014)0219 [2014].
[33] art 4a Resolution of 12 March 2014, P7_TA(2014)0219, entitled 'access to data initially processed for purposes others than those referred to in article 1(1)'.
[34] ibid, art 4a(1)(a)-(d).
[35] ibid, art 4a (2).
[36] As defined in Art 3(7) Directive 2016/680.
[37] As described in art 1(1) Directive 2016/680, ie for 'the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding of threats to public security.'

## III. Regime of Purpose Limitation under Directive 2016/680

This section describes the principle of purpose limitation in Directive 2016/680 and compares it with the regime established under the GDPR. It also discusses the nature and content of Article 4(2) of the new Directive, which provides the conditions of further processing of personal data collected for a different purpose.

### 1. Comparison with the GDPR Regime

As noted in Section II, the principle of purpose limitation is sub-divided into a principle of *purpose specification* and a principle of *compatible use*.[38] According to Article 4(1) of Directive 2016/680, personal data are 'collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.' The principle is worded in identical terms in Article 5(1) GDPR. However, as explained below, the principle is interpreted differently.

The *purpose specification* principle focuses on the initial purpose of collection. As observed by the Article 29 Working Party (A29WP),[39] 'law enforcement, *per se*, shall not be considered as one specified, explicit and legitimate purpose.'[40] Each purpose needs to comply with the three criteria of specificity, explicitness, and legitimacy. In the scenarios under review in this paper, the original purpose of data collection is not a law enforcement purpose. It can be a commercial, an administrative or an operational purpose, and in general, any non-law enforcement purpose falling within the scope of the GDPR. Only the purpose of the subsequent use is a law enforcement purpose covered by Directive 2016/680.

The second principle, *compatible use*,[41] entails that personal data collected for a specific purpose are used following that purpose. They should not be further processed in a way incompatible with the initial purpose of processing. What does this principle mean in the context of Directive 2016/680? First, it would be wrong to conclude that unrelated purposes are necessarily incompatible. For example, under the GDPR, the subsequent use of personal data for research or archive purposes is not considered incompatible with the original purpose of collection.[42] Second, two law enforcement purposes are not necessarily compatible because they belong to the same field.[43] It is, therefore, necessary to assess the

[38] A29WP, 'Opinion 03/2013 on purpose limitation' [2013] WP203.
[39] A29WP is an independent advisory body to the European Commission on data protection matters, see <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083> accessed 10 April 2018; it will be replaced by the European Data Protection Board (art 68 et seq GDPR).
[40] A29WP, 'Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' [2015] WP233, 6.
[41] In other instruments, such as in the OECD Privacy Guidelines (n 16), the principle is described as 'use limitation'.
[42] art 5(1)(b) GDPR.
[43] See EDPS, 'Opinion of the European Data Protection Supervisor on the Data Protection Reform Package' [2012], para 334 states: 'it should be clear that within the law enforcement context different purposes can be

compatibility between the purposes to determine their compatibility. Before the adoption of the new data protection framework, in cases where personal data were first collected for a non-law enforcement purpose and further used for a law enforcement purpose, the A29WP recommended the application of several factors to assess their compatibility.[44] Those factors have been incorporated in the GDPR[45] but are absent from Directive 2016/680. Last, 'irrespective of the compatibility of purposes,' Article 6(4) GDPR provides two legal grounds for the further processing: the data subject's consent and a national or EU law, which is 'necessary and proportionate' to protect specific interests identified in Article 23 GDPR.[46] The provision does not state that Article 23 GDPR constitutes a legal ground to process data for incompatible purposes but only that a law, which is 'necessary and proportionate …to safeguard the interests *referred to* in Article 23(1)' constitutes such a legal basis.[47]

The approach followed by Directive 2016/680 is different. Article 4(2) of Directive 2016/680 only sets out the conditions under which further processing for a purpose other than the original purpose of collection is allowed. In particular, it provides that:

> Processing by the same or another controller for any of the purposes set out in Article 1(1) other than for which the personal data are collected shall be permitted in so far as:
> 1. the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and
> 2. processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.



The scope of the initial processing and the conditions of the further processing are addressed in the next sub-sections.

### 2. Scope of the Initial Processing

The wording of Article 4(2) in respect to the context of the initial processing is ambiguous. The provision only mentions the initial purpose of processing as a purpose 'other than for which the personal data are collected.' Article 4(2) does not state whether the initial purpose falls within or outside the scope of Directive 2016/680. The provision does not even make a link between the principle of purpose limitation [defined in Article 4(1) of the Directive] and the conditions applicable to the further processing. One understands that the two are linked through Recital 29 of the Directive. The recital describes together the principle of purpose limitation and the conditions applicable to the further processing for

incompatible' <https://edps.europa.eu/sites/edp/files/publication/12-03 07_edps_reform_package_en.pdf > accessed 10 April 2018.

[44] Opinion 03/2013 (n 38), examples about Eurodac, PNR.

[45] art 6(4) GDPR.

[46] Those interests include public security, but also the prevention, investigation or prosecution of criminal offences or the protection of individuals, see art 23(1)(a)-(j) GDPR.

[47] Emphasis added.

a different purpose. Based on that recital, one could claim that Article 4(2) only applies to the further processing of personal data initially collected for a law enforcement purpose. However, because a recital is a non-binding provision,[48] one could also argue that Article 4(2) can apply to the further processing of personal data collected outside the scope of Directive 2016/680.

This ambiguity is problematic because it has consequences for the status of the subsequent use of GDPR data for a law enforcement purpose. If Article 4(2) of Directive 2016/680 does not apply to the further processing of GDPR data, there is an uncertainty on the qualification of this subsequent processing operation. Should it be considered as initial processing under Directive 2016/680? During the negotiations on the draft Police and Criminal Justice Directive, the European Commission opined that such processing should be considered as 'initial processing' of 'police or criminal justice' data instead of further processing.[49] The European Commission believed that 'the further processing across the two legal instruments would create problems,' thus 'there were no specific articles [in the draft Directive] to be used for that.'[50] As a consequence, following this interpretation, the further processing of GDPR data would neither be subject to the principle of purpose limitation, as defined in Article 4(1) of the Directive, nor be subject to the conditions applicable to further processing set out in Article 4(2) of the Directive. The situation does not seem, however, to be that simple. No recital or provision in both the GDPR and Directive 2016/680 confirms the European Commission's views.[51] Both texts are actually silent on that matter. Because of the ambiguous wording of Article 4(2) of Directive 2016/680, it could be argued that both hypotheses can be envisaged.

The conditions under which Article 4(2) allows further processing are analysed next.

### 3. Article 4(2) of Directive 2016/680 as Derogation from the Principle of Purpose Limitation?

Article 4(2) of the Directive allows the further processing under the conditions of legality [Article 4(2)(a)] as well as necessity and proportionality [Article 4(2)(b)]. However, these conditions are not linked, implicitly or explicitly, to any compatibility requirement. The

[48] Recitals are, however, interpretative tools; see Roberto Baratta, 'Complexity of EU law in the domestic implementing process' (Speech at the 19th Quality of Legislation Seminar 'EU Legislative Drafting: Views from those applying EU law in the Member States', 3 July 2014) <http://ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf > accessed 10 April 2018.

[49] The European Commission specified that 'if a legal obligation to transfer data to the police existed, such a transfer would be considered as an initial police processing' in fn 118 of Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, chs II and III, to delegations, 14 April 2015, doc 7740/15 [2015] <http://www.statewatch.org/news/2015/apr/eu-council-dp-directive-chap-II-7740-15.pdf> accessed 10 April 2018.

[50] ibid.

[51] One could add that statements made by the European Commission, as well as by other EU institutions, during the negotiation process of a legislative instrument have no legal binding value in the absence of reference to these statements in the instrument itself, see Case C-292/89 *R v Immigration Appeal Tribunal ex parte Gustaff Desiderius Antonissen* [1991] ECR-I-745, para 18.

term is absent from the provision. By comparison, Article 3(2) of the Council Framework Decision 2008/977/JHA, now replaced by Directive 2016/680, only applies to purposes 'not incompatible' with the purpose of collection.[52] Thus, it seems that Article 3(2) of the Framework Decision was drafted as an interpretation of the principle of purpose limitation as it only authorises further processing 'not incompatible.'

Concerning Article 4(2) of Directive 2016/680, it should be mentioned that during the negotiations on the draft Police and Criminal Justice Directive, Member States were split on its scope: some wanted to define specific rules applicable to the further processing for compatible purposes; others rules applicable to incompatible purposes.[53] In the end, the adopted text refers to neither. The definition of 'compatible purposes' is thus left at the national level.[54] As a consequence, in the absence of compatibility requirement, it can be deduced that Article 4(2) of Directive 2016/680 applies 'irrespective of the compatibility between the purposes.' As such, the provision constitutes an exception to the principle of purpose limitation and differs from Article 3(2) of the Framework Decision.

Next, if Article 4(2) of Directive 2016/680 is construed as a derogation from the principle of purpose limitation, it is argued that it should be interpreted in accordance with the Charter of Fundamental Rights [Article 52(1) of the Charter] and the European Convention on Human Rights [Article 8(2) ECHR].[55]

#### *a. Lower Standard of Protection?*

As specified in the GDPR, restrictions on data subjects' rights and on the corresponding data protection principles should apply 'in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.'[56] One could add that the requirements have to be understood as interpreted by the CJEU and the European Court of Human Rights (ECtHR).



Directive 2016/680 does not contain a similar provision. It only provides, in Recital 46, that 'any restrictions of the rights of the data subject' must be in accordance with both the Charter and the ECHR. Thus, restrictions on data protection principles are not expressly subject to the same requirements. It is argued here that, as worded, Directive 2016/680

[52] art 3(2) Framework Decision reads as follows: 'Further processing for another purpose shall be permitted in so far as: (a) it is not incompatible with the purposes for which the data were collected…'; this requirement of 'non-incompatibility' can also be found in Principle 5 of the Council of Europe's Recommendation R(87)15.
[53] See discussions among Member States, and in particular the position of Sweden opposed to limit the rules on the further processing to compatible purposes whereas the Czech Republic supported rules applicable to purposes 'not incompatible' with the initial purpose of processing; respectively fns 151 and 152 of Delegations Document on the draft proposal Directive, Council of the European Union, 10335/15, 29 June 2015.
[54] Even if this is not expressly mentioned in Directive 2016/680; by comparison, see Recital 6 Council Framework Decision that explicitly specifies 'the Framework Decision should leave it to Member States to determine more precisely at national level which other purposes are to be considered incompatible with the purposes for which the personal data were originally collected.'
[55] art 52(1) Charter is a general limitation clause, whereas art 8(2) ECHR is a specific limitation clause applying only to interferences with the right to privacy.
[56] Recital 73 GDPR read together with art 23 GDPR; as previously observed, one could still wonder whether any data subject's rights can be derived from the principle of purpose limitation (see, n 15).

provides for a lower standard of protection than the GDPR. However, since the principle of purpose limitation is a component of the fundamental right to data protection, derogation from that principle should, in any event, be interpreted according to the case law of the CJEU and the ECtHR.

### *b. Interpretation of the Derogation*

The right to the protection of personal data, enshrined in Article 8 of the Charter, expressly refers to the principle of purpose limitation as one of its constitutive elements. Article 8, paragraph 2, specifies that personal data 'must be processed fairly for specified purposes.'

Following Article 52(1) of the Charter, restrictions on fundamental rights should comply with the following conditions: be 'provided by law', 'respect the essence of the rights' at stake, be 'subject to the principle of proportionality' and 'necessary and genuinely meet the objectives of general interest' or 'the need to protect the rights and freedoms of others.'

As analysed by Lynskey,[57] the requirements of legality, proportionality, and necessity set out in Article 52(1) can be rooted in the case law of the ECtHR, whereas the requirement of 'respect for the essence of the right' is new.[58] Thus the legality, necessity and proportionality requirements, provided by Article 4(2) of Directive 2016/680 should be understood as interpreted by both the ECtHR and the CJEU.

*i. Legality, Necessity, and Proportionality*

First, concerning the legality principle, formulated as 'in accordance with the law', Directive 2016/680 indicates that the principle should be understood as interpreted by the two Courts.[59] The Directive is, however, silent on the interpretation of the principles of necessity and proportionality, which are worded in general terms in Article 4(2) of Directive 2016/680. By comparison, the GDPR makes more explicit references to the case law of the ECtHR when it describes the principles as 'necessary and proportionate in a democratic society'.[60] This wording refers in particular to the requirement of necessity set out in Article 8(2) ECHR, where any interference with the right to privacy has to be 'necessary in a democratic society'.[61] Article 8 ECHR pertains to the right to privacy, which encompasses the right to the protection of personal data as interpreted by the ECtHR.[62] As

[57] Orla Lynskey, *The Foundations of EU Data Protection Law* (OUP 2015), ch 5, 172.
[58] Brkan explains, however, that the requirement of essence can find its origin in several Member States' Constitutions, see Maja Brkan, 'In Search of the Concept of Essence of EU Fundamental Rights through the Prism of Data Privacy' (2017) 2017-01 Maastricht Faculty of Law Working Paper 1, 5-10.
[59] Recital 33 Directive 2016/680.
[60] art 6(4) GDPR.
[61] The ECtHR has added the criterion of proportionality in its interpretation of Art 8(2) ECHR; eg Douwe Korff, 'The Standard Approach under articles 8-11 ECHR and article 2 ECHR' (2009) <http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf > accessed 10 April 2018.
[62] eg *S and Marper v United Kingdom* Apps nos 30562/04 and 30566/04 (ECHR, 4 December 2008), para 103 where the ECtHR states: '[t]he protection of personal data is of fundamental importance to a person's

such the case law of the ECtHR - as far as it relates to the protection of personal data as part of the right to privacy - is also relevant to the interpretation of the right to the protection of personal data.[63]

*ii. Essence of the Right*

Second, on the requirement of 'respect of the essence of the right',[64] very little case law is available on what constitutes the 'essence' of the fundamental right to data protection. Only in *Schrems* did the Court find a violation of the essence of the right to privacy (but not of the right to data protection).[65] In more recent decisions, *Digital Rights Ireland* and *Tele2 Sverige*, the Court checked whether the Data Retention Directive and national data retention measures violated the essence of the right to data protection. Based on the existence of data security provisions, the Court concluded there was no violation of the essence of the right to data protection.[66] This reasoning prompted some authors to argue that

> [t]he Court is therefore perhaps suggesting that the essence of the right to data protection is not an *objective* of that right (such as privacy protection or individual control over personal data) but rather it is the *means* of achieving data protection that constitutes the essence of the right.[67]

Interestingly in Opinion 01/2015 on the proposed agreement between the EU and Canada on passenger name record (PNR) data,[68] the Court seemed to admit that the proposed agreement does not violate the essence of the right to data protection because it contains 'rules intended to ensure, inter alia, the security, confidentiality and integrity of that data, and to protect against unlawful access and processing.'[69] Thus, the Court seems to include the principle of purpose limitation (or at least its objective) within the scope of 'the essence' of the right to data protection.



As a consequence, the test of legality, necessity, and proportionality, set out in Article 4(2) of Directive 2016/680 should be interpreted according to the case law of the Courts on respectively Article 52(1) of the Charter and Article 8(2) ECHR. The characteristics of the different tests are illustrated in the next section with case law. Since Article 4(2) of Directive 2016/680 is understood as an exception to the principle of purpose limitation,

enjoyment's of his or her right to respect for private and family life, as guaranteed by article 8 of the Convention.'

[63] On the relationship between the right to privacy and the right to the protection of personal data, see Lynskey (n 57) ch 4, 89-130.

[64] See also Brkan (n 58) 13.

[65] Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, para 94, where the Court found that 'permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.'

[66] *Digital Rights Ireland* (n 3) para 40.

[67] Lynskey (n 57) ch 5, 171.

[68] *Opinion 1/15 (*n 28)

[69] ibid para 150.

measures allowing the subsequent use of personal data should also be assessed in respect of their impact on the 'essence of the fundamental right' to data protection.

Building on the ambiguous wording of Article 4(2) of Directive 2016/680, Section IV suggests a reading of the provision that would encompass the further processing of GDPR data.

## IV. Further Processing of GDPR Data Falling within the Scope of Article 4(2) of Directive 2016/680

As explained in the introduction, the article discusses the role of the principle of purpose limitation when GDPR data are re-used for one of the purposes of Directive 2016/680. When the processing activities are carried out across the two instruments, no specific role seems to have been assigned to the principle of purpose limitation. For illustration purposes, one could refer to the examples provided in the introduction on the further processing of personal data: the case of law enforcement access and further use of biometric data held by social networks, employers or schools for administration purposes.

Based on other authors' analysis,[70] this section suggests a different approach to the principle of purpose limitation focusing on the subsequent use of personal data. Article 4(2) of Directive 2016/680 seems to follow this approach as it regulates the conditions of further processing, irrespective of the compatibility between the purposes. Thus, the article proposes a reading of Article 4(2) that would apply to personal data initially collected for a purpose within or outside the scope of the Directive. To control how law enforcement authorities further use GDPR data, the article suggests tying the principle of purpose limitation to the accountability obligation of law enforcement authorities (i.e. Article 19 of Directive 2016/680).

### 1. Focus on the Regulation of Data Use instead of Data Collection?

It could be argued that the principle of purpose limitation has not been forgotten, but its application in the specific scenario of reprocessing GDPR data for a law enforcement purpose is left to the discretion of Member States. This interpretation would, however, not be consistent with the fundamental nature of the principle. Thus, it seems difficult to bypass the principle. But since the new technological environment did not exist at the time the principle was first adopted, some authors have questioned its applicability as initially conceived.

In the context of big data, Morel and Prins have shown the inadequacy of the principle with the mass-collection of personal data and propose instead a test based on legitimate

[70] In the context of big data and big data analytics.

interests.[71] If the principle of purpose limitation is not adapted to big data,[72] it is, however, questionable if it could be replaced by a test based on the legitimate interests of data controllers, as suggested by the authors. More interesting in the context of this paper are the arguments brought forward by Coudert on the application of the principle of purpose limitation in the field of law enforcement cooperation. In a well-argued article, Coudert analyses the provisions on purpose limitation in the new Europol Regulation.[73] According to Coudert, the Europol Regulation moves towards a different approach to the principle of purpose limitation in the context of big data analytics in the criminal field. In her view, the traditional approach of the principle that she describes as a 'silo-based' approach – referring to the separation of data in distinct databases – is replaced by 'the regulation of legitimate data uses'.[74] However, as she explains, the Europol Regulation falls short on the practical implementation of this new approach.[75] To control the use of personal data by data controllers and restrict further processing, Coudert suggests relying on privacy by design obligations and on the oversight by national data protection authorities.[76]

In the current article, the context of processing does not focus on big data analytics but on the subsequent use of GDPR data in the context of criminal investigations[77] or criminal surveillance.[78] The interpretation suggested by other scholars might, thus, not be entirely suitable. Instead, the paper focuses on the breadth of Article 4(2) of Directive 2016/680. The next subsection suggests a reading of the provision that would apply to any initial processing. As such, the further processing of GDPR data would be subject to Article 4(2) of Directive 2016/680.

### 2. Interpretation of Article 4(2) to Encompass Subsequent Uses of GDPR Data

Based on the findings of the previous section, the article attempts to provide an interpretation of the legality, necessity and proportionality of the subsequent use of GDPR data for a law enforcement purpose. Since Article 4(2) of Directive 2016/680 is



[71] eg Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis, Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (SSRN, 25 May 2016) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123> accessed 10 April 2018.

[72] Big data challenges indeed the principle of purpose limitation and other data protection principles, see Christopher Kuner et al, 'The Challenge of "Big Data" for Data Protection' (2012) 2(2) International Data Privacy Law 47; as well as Ira Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3(2) International Data Privacy Law 74.

[73] Europol Regulation (n 23).

[74] Coudert (n 28) 4.

[75] ibid.

[76] ibid 10-12.

[77] Criminal investigation usually starts with an offence and falls within the criminal procedural framework.

[78] Criminal surveillance is not linked to a specific offence but to 'risks and threats to security', it is generally used to anticipate or prevent criminal offences; depending on the countries, criminal surveillance is covered or not by the criminal procedural framework, see John AE Vervaele, 'Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reloading Data Protection* (Springer 2014) 115-116. The distinction between criminal investigation and criminal surveillance is not always clear-cut, in particular, criminal surveillance can be used in a context of criminal investigation and target specific individuals, see Ira Rubinstein, Gregory Nojeim and Ronald Lee, 'Systematic Government Access to Private-Sector Data, A Comparative Analysis' in Fred Cate and James Dempsey (eds), *Bulk collection, Systematic Government's Access to Private-Sector Data* (OUP 2017) 38-42.

interpreted as derogation from the principle of purpose limitation, the article also discusses whether and how the 'essence of the right' should be added as an extra criterion.

### *a. 'In Accordance with the Law'*

The first condition 'in accordance with the law' sets up the legality requirement. Extensively interpreted by the ECtHR,[79] the term 'law' is broadly understood and does not need to result from a legislative procedure.[80] The law needs, however, to be clear, accessible and foreseeable.[81] The legality requirement does not call for many remarks. On the foreseeability aspect one could, however, observe that the ECtHR has introduced nuances taking into account the context of the interference. In a general context, a foreseeable law is a law, which is 'formulated with sufficient precision to enable any individual –if need be with appropriate advice – to regulate his conduct.'[82] A law is for instance sufficiently precise if it describes its scope; provides safeguards to ensure the security, confidentiality, and safety of the data; and details how the data are stored, retained and further used. Those examples originate from case law on the retention and storage of biometric and DNA data for criminal purposes.[83] In the context of police-led surveillance (such as interceptions of communications)[84] or secret surveillance in the interest of national security,[85] the ECtHR has established a different standard. Foreseeability in those contexts 'cannot mean that an individual should be enabled to foresee precisely what checks will be made.' Instead, the law should be clear enough to give an 'appropriate indication' as to the 'circumstances' and 'conditions' under which surveillance measures are allowed.[86]

In the case of subsequent use of GDPR data for law enforcement purposes, the legality requirement could imply the existence of a national criminal procedural law that would detail the conditions under which personal data can be requested, accessed and further used. If the data are necessary for surveillance purposes, the national law would have to provide an 'adequate indication' as to the 'circumstances' and 'conditions' under which surveillance measures are allowed. According to the ECtHR, the law must contain specific safeguards, which include 'procedure to be followed for examining, using and storing the obtained data.'[87]

[79] eg *Malone v UK* App no 8691/79 (ECHR, 2 August 1984), paras 66-68; *Rotaru v Romania* App no 28341/95 (ECHR, 4 May 2000), para 52; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* App no 62540/00 (ECHR, 28 June 2007), para 71.
[80] Recital 33 Directive 2016/680.
[81] eg *Malone* (n 79) para 67.
[82] eg *Rotaru* (n 79) para 55; but also, *S and Marper* (n 62) para 95.
[83] *S and Marper* (n 62) para 99.
[84] eg *Malone* (n 79).
[85] eg *Leander v Sweden* App no 9248/81 (ECHR, 26 March 1987).
[86] eg *Malone* (n 79) para 67 as cited for example in Leander (n 85) para 51 and *Amann v Switzerland* App no 27798/95 (ECHR, 16 February 2000) para 56.
[87] *Weber and Saravia v Germany* App no 54934/00 (ECHR, 29 June 2006), para 95.

On its side, the CJEU interprets the legality requirement by reference and analogy to the case law of the ECtHR on Article 8 ECHR.[88] As a consequence, a national or EU legislation must 'lay down clear and precise rules' on the 'scope' and 'application' of the measure and provide 'minimum safeguards' to prevent abuses, such as 'unlawful access and use' of data in the cases of data retention. The same conditions apply irrespective of the field, whether or not it falls within the scope of law enforcement.

In conclusion, under Article 4(2)(a) of Directive 2016/680, a legality test should be performed. That would imply checking if a specific national law (e.g. a national criminal procedural law) allowing law enforcement authorities (e.g. police authorities) to further process personal data held by third parties contains the elements described by the courts.

The two other requirements, proportionality and necessity, are more subjective than the legality requirement. They are dealt with separately, but as pointed out by the European Data Protection Supervisor (EDPS), they overlap and could 'be carried out concurrently or even in the reverse order.'[89] However, the order followed here is the one provided by Article 4(2) of Directive 2016/680. It is fair to say that due to the order if the measure has not passed the 'test of necessity', the principle of proportionality should not be assessed.[90]

#### *b. 'Necessary to that Other Purpose'*

The ECtHR and the CJEU have issued slightly different tests of necessity. According to the ECtHR, 'necessity' refers to a measure that 'is necessary in a democratic society.'[91] In the context of the protection of personal data, this means that a measure answers 'a pressing social need' to meet the necessity requirement.[92] Member States benefit from a margin of appreciation to determine the existence of a 'pressing social need'.[93] The protection of national security constitutes, for instance, a pressing social need.[94] As analysed by the A29WP, the test of 'pressing social need' is defined by the 'context' of the measure and 'evidence' of the necessity of such a measure for society.[95] As a consequence, the ECtHR only applies a test of strict necessity if the circumstances of the interference require it. In



[88] eg *Digital Rights Ireland* (n 3) para 54; Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and others* [2016] ECLI:EU:C:2016:970, para 109.
[89] EDPS, 'Assessing the necessity of measures that limit the fundamental right to data protection: A toolkit' [2017] <https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf > accessed 10 April 2018.
[90] ibid 5.
[91] See *Handyside v UK* App no 5493/72 (ECHR, 7 December 1976), para 48 where the Court described 'necessity' in the following terms 'whilst the adjective "necessary"…is not synonymous with "indispensable"…, "the words absolutely necessary" and "strictly necessary"…neither has it the flexibility of such expressions as "admissible", "ordinary", …"useful", "reasonable"…or "desirable."'
[92] eg *S and Marper* (n 62) para 101; for further details see Steven Greer, 'Exceptions to Article 8 to 11 of the European Convention on Human Rights' (1997) <http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf> accessed 10 April 2018.
[93] This margin depends on 'the nature of the legitimate aim pursued' and 'on the nature of interference at stake', see *Connors v the United Kingdom* App no 66746/01 (ECHR, 27 May 2004), para 82.
[94] *Leander* (n 85) para 59.
[95] A29WP, 'Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector' [2014] WP211.

the context of 'secret surveillance', the Court ruled in particular that interference had to meet the criteria of 'strict necessity.'[96]

As for the CJEU, the Court has developed a test of 'strict necessity' in its case law on Articles 7 and 8 of the Charter of Fundamental Rights. The test of necessity applies even in the context of law enforcement or in relation to surveillance measures.[97] According to the EDPS,

> the requirement of 'strict necessity' flows from the important role the processing of personal data entails for a series of fundamental rights, including freedom of expression. Even if specific rules are adopted in the field of law enforcement, for instance, Directive 2016/680, this does not justify a different assessment of necessity.[98]

One could get inspiration from the toolkit developed by the EDPS on the test of necessity to guide the EU institutions before the adoption of new legislative measures. Based on the case law of the CJEU and the ECtHR, the test of necessity requires a 'factual' analysis, the identification of the fundamental rights impaired, the objective of the measure and the 'less intrusive' option to achieve the same goal.[99] Transposed to a measure allowing the subsequent use of GDPR for a law enforcement purpose, the test of necessity would require going through the four steps. First, the factual assessment of the further processing could determine whether the processing is strictly necessary to the law enforcement purpose. That would imply identifying the purpose, such as criminal investigation or criminal surveillance (and whether targeted or not). Different factors could be taken into account such as the individuals impacted by the further processing (suspects, witnesses, victims or citizens); the type of data processed (sensitive data or personal data); the kinds of processing operations as well as the persons who have access to the processed data. An assessment of impacts on data subjects' rights should also be carried out, and in particular how individuals will be able to exercise their right to remedy. Finally, it might be essential to consider the initial context of processing, especially when data are further used for criminal surveillance.

#### *c. 'Proportionate to that Other Purpose'*

As observed by some authors, it might be difficult to distinguish the test of necessity from the test of proportionality.[100] Advocate General Maduro wrote in *Huber* that 'the concept of necessity…is well established as part of the proportionality test.'[101] In a narrow sense, however, the test of proportionality refers to 'proportionality stricto sensu'. According to

[96] *Szabó and Vissy v Hungary* App no 37138/14 (ECHR, 12 January 2016), para 73.
[97] eg *Digital Rights Ireland* (n 3); *Tele2 Sverige* (n 88), and *Schrems* (n 65).
[98] EDPS (n 89) 7.
[99] EDPS (n 89).
[100] Steve Peers and Sacha Prechal, 'Article 52' in Steve Peers et al (eds), *The EU Charter of Fundamental Rights, A Commentary* (Hart Publishing 2014), 1480
[101] Case C-524/06 *Heinz Huber v Bundesrepublik Deutschland* [2008] ECLI:EU:C:2008:194, Opinion of AG Maduro, para 27.

the CJEU, proportionate measures are 'appropriate' in relation to their objectives and 'do not go beyond what is necessary'.[102] The analysis of what constitutes a measure that 'would go beyond what is necessary' is very factual. For example, the CJEU has relied on the existence of 'specific guarantees' to ensure that the processing of sensitive data (such as fingerprints) was 'effectively protected from misuse and abuse'.[103]

Concerning the subsequent use of GDPR data for a law enforcement purpose, the proportionality of the measure might be assessed taking into account existing safeguards (such as limited storage of data in an identifiable form, description of uses, procedures to preserve the confidentiality, security, and integrity of the data).[104]

#### *d. Missing Criterion: Respect of the Essence of the Fundamental Right to Data Protection?*

As explained, the requirement of 'respect of the essence of the right' is a condition imposed by Article 52(1) of the Charter on the limitations to fundamental rights. Yet, if as argued in the previous section, Article 4(2) of Directive 2016/680 is construed as an exception to the principle of purpose limitation, its application should comply with the requirements of the Charter and the ECHR as respectively interpreted by the CJEU and the ECtHR. On the constitutive elements of the 'essence of the right' to data protection, few details are available. However, as mentioned in the previous section, in Opinion 1/15, the CJEU established the 'protect[ion] against unlawful access and processing' as an element of the essence of the right.[105]

The criterion of 'essence of the right' is absent from Article 4(2) of Directive 2016/680. If it is accepted that the provision should be interpreted in compliance with Article 52(1) of the Charter, the essence criterion should also be assessed.



### 3. Accountability of Law Enforcement Authorities as Additional Safeguard?

Last, as already suggested,[106] a different approach to the principle of purpose limitation should be supported by additional safeguards. Article 19 of Directive 2016/680 sets out the accountability of law enforcement authorities to enable them to demonstrate compliance with their data protection obligations. As worded,[107] the principle of accountability relates to the obligation that law enforcement authorities have to comply with their data protection obligations.

Even if the provision is vague, it ties the obligation of accountability to the implementation of appropriate technical and organisational measures, such as the obligation of 'data protection by design'. That could include the adoption of policies describing the legality,

[102] eg Case C-291/12 *Michael Schwarz v Stadt Bochum* [2013] ECLI:EU:C:2013:670, para 40.
[103] ibid para 55 et seq, referring to *S and Marper* (n 62) para 103.
[104] eg *S and Marper* (n 62) para 99.
[105] *Opinion 1/15* (n 28) para 150.
[106] Coudert (n 28).
[107] art 19 Directive 2016/680.

necessity and proportionality assessment of the subsequent use of GDPR data and the impacts on data subjects.

In the next section, the hypothesis following which the subsequent use of GDPR data falls outside the scope of Article 4(2) of Directive 2016/680 is addressed.

## V. Shortcomings: Consequences of Subsequent Uses of GDPR Data outside the Scope of Article 4(2) of Directive 2016/680

In that section, Article 4(2) of Directive 2016/680 is considered as applying exclusively to the further processing of personal data initially collected for one of the purposes of Directive 2016/680.

This interpretation, favoured by the European Commission,[108] will most likely prevail among Member States. As a matter of illustration, several Member States have already decided to clear up the ambiguity in their draft implementing laws. For example, both the UK and the Dutch draft laws specify the nature of the initial purpose of collection. In the United Kingdom, Section 34 of the Data Protection Bill defines the principle of purpose limitation and restricts the rules on the further processing to personal data 'collected for a law enforcement purpose.'[109] The Dutch draft law suggests a similar implementation of Article 4(2) of the Directive since the rules on the further processing will only apply to 'police' data ('*politiegegevens*').[110]

### 1. Subsequent Use of GDPR Data as 'Initial Processing' under the Directive?

Following the analysis made in the previous sections, the subsequent use of GDPR data falls within the remit of Directive 2016/680 but is not expressly included into the scope of Article 4(2) of the Directive. In case Article 4(2) exclusively applies to the further processing of personal data initially collected in a law enforcement context, does it mean that the further processing of GDPR data is considered as initial processing of 'police' data under the Directive? If so, what are the consequences?

First of all, such an interpretation does not seem to be in line with the positions defended by the EDPS and the A29WP on various occasions. They both reiterated the importance of the principle of purpose limitation in scenarios where personal data were accessed and further used by law enforcement authorities for a purpose unrelated to the initial purpose

[108] See the position of the European Commission (n 49); it also seems consistent with Recital 29 of the Directive (n 48).
[109] See section 36 (1)-(3) of the UK Data Protection Bill, 22 https://publications.parliament.uk/pa/bills/cbill/2017-2019/0190/18190.pdf accessed 10 April 2018.
[110] Dutch Draft law, art 3 <https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel:34889> accessed 10 April 2018.

of collection.[111] In particular, they have issued opinions in the context of the PNR Directive, the repurposing of Eurodac data for law enforcement purposes, and during the negotiations of the new data protection framework.[112] For instance, concerning the proposal for a PNR Directive, the EDPS criticized the lack of objective criteria to limit the access to and the subsequent use of the PNR data by law enforcement authorities. The EDPS found that the purposes for which the data could be re-used had not been precisely identified.[113] Similar critics were formulated about the recast of the Eurodac database, originally constituted to manage asylum applications among Member States. In 2012 already, the EDPS found that the extension of the scope of the database for law enforcement purposes was 'difficult to reconcile with the purpose limitation principle, which is one of the key principles of data protection law.'[114] The EDPS also opined that 'the assessment as to the necessity and proportionality of the creation of the Eurodac would have been completely different if law enforcement access was envisaged from the outset.'[115]

Second, this qualification has consequences on the determination of the applicable regime. As explained in the previous section, further processing of 'police' data for a different law enforcement purpose is subject to the conditions of legality, necessity and proportionality set out in Article 4(2) of the Directive. The question that arises is whether the rules imposed on the initial processing are similar to the ones applicable to the further processing, i.e. whether the initial processing under Directive 2016/680 is also subject to conditions of legality, necessity, and proportionality. The rules applicable to initial processing under the Directive are therefore assessed.



According to Article 8 of Directive 2016/680,[116] a processing operation is lawful if it is 'necessary for the performance of a task carried out by a competent authority' for one of the purposes of the Directive and 'is based on Union or State law.' An initial processing operation is, thus, also subject to a legality requirement. This requirement is understood

[111] eg A29WP, Opinion 03/2013 (n 38); EDPS, 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the citizen' [2009] OJ C276/09, para 41.
[112] eg EDPS, 'Opinion 5/2015, Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2015] <https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf> accessed 10 April 2018.
EDPS, 'Opinion 07/2016, EDPS Opinion on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations)' [2016] <https://edps.europa.eu/sites/edp/files/publication/16-09-21_ceas_opinion_en.pdf > accessed 10 April 2016.
[113] EDPS, Opinion 5/2015 (n 112) paras 25-27.
[114] EDPS, 'Opinion on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No[…][…](Recast version) [2012], para 28 <https://edps.europa.eu/sites/edp/files/publication/12-09-05_eurodac_en.pdf > accessed 10 April 2018.
[115] ibid para 27.
[116] art 8 Directive 2016/680 entitled 'lawfulness of processing.'

as interpreted by the ECtHR and the CJEU, i.e. the law must be clear, accessible and foreseeable.[117]

Article 8 also provides for a condition of necessity. However, that condition is different from the test of necessity under Article 4(2) of Directive 2016/680. As observed by the EDPS, the condition of 'necessity' can be a requirement for the 'lawfulness of the processing' as well as a condition applicable to the restrictions on fundamental rights. However, the two concepts of necessity are distinct.[118] As explained in the previous section, the condition of necessity referred to in Article 4(2) of Directive 2016/680 should be interpreted as a condition of strict necessity. This results from the case law of the CJEU on the application of Article 52(1) of the Charter on interferences with the right to data protection. Therefore, on the necessity requirement, initial processing does not seem to be subjected to the same test as further processing.

An initial processing operation must also comply with the criteria set out in Article 4(1) of the Directive, i.e. the data protection principles applicable to any processing. Among the different principles, the one described in Article 4(1)(c) is of particular interest. It relates to the principle of data minimisation in the context of law enforcement. As such, it requires the processing of personal data 'not to be excessive in relation to [their] purposes.' It could be argued that the provision only provides a mild obligation of proportionality since the criterion used to determine the amount of data collected ('not excessive') is less precise than the requirement of proportionality imposed by the courts ('not beyond what is necessary'). As such, the obligation of proportionality applicable to the initial processing [Article 4(1) of the Directive] is not identical to the one applicable to the further processing [Article 4(2) of the Directive].

In conclusion, the conditions of necessity and proportionality to which an initial processing operation would be subject are not comparable to the conditions set out in Article 4(2) of the Directive, as interpreted in this article. Likewise, an initial processing operation is not subject to the requirement of 'respect of essence of the right.' Last, one might wonder if considering a subsequent use of GDPR data as initial processing of 'police' data would not impair the fundamental right to data protection since the principle of purpose limitation is one of its constitutive elements.[119]

### 2. Consequences on Data Subjects' Rights

Finally, there is a critical shortcoming linked to the regulation of data processing through two distinct instruments. Data subjects whose personal data are first collected for a GDPR

[117] Recital 33 Directive 2016/680 to be read together with art 8 Directive 2016/680.
[118] EDPS, 'Developing a "Toolkit" for Assessing the Necessity of the Measures that Interfere with Fundamental Rights' (Background Paper for consultation [2016], 4 <https://edps.europa.eu/sites/edp/files/publication/16-06-16_necessity_paper_for_consultation_en.pdf> accessed 10 April 2018.
[119] art 8(2) Charter.

purpose have specific rights attached to that processing operation.[120] However, if their data are further used in a law enforcement context, they do not benefit from the same safeguards. In particular, they are not informed that their data have been further processed for law enforcement purposes. The nature of law enforcement activities obviously requires some adjustments in respect of data subjects' rights to protect on-going investigation for example. However, the current right to information set out in Article 13 of Directive 2016/680 only imposes an obligation to make specific information *available* to individuals. It does not, expressly, provide for an obligation to notify individuals about the processing of their personal data. Yet, according to the CJEU's case law,[121] individuals whose personal data have been accessed by law enforcement authorities should be notified once the investigations are over or can no longer be jeopardised. The purpose of the notification is to allow individuals to exercise their right to remedy.[122]

One could claim that a national law that would inform individuals about the possible access to and further use of their personal data by law enforcement authorities would not be sufficient in light of the CJEU's case law.[123] Transparency about a possible processing operation is not the same as notification of an actual processing operation. As argued elsewhere,[124] it might be necessary to interpret Article 13 of Directive 2016/680 as obliging Member States to adopt national laws to notify individuals about the access to and subsequent use of their personal data by law enforcement authorities. On this specific issue, the Council of Europe seems to follow this approach in its 'practical guide in the use of personal data in the police sector.'[125] The report emphasizes that

> even if restrictions or derogations to the right to information were applied, information should be provided to the data subjects as soon as it no longer jeopardises the purpose for which the data were used.[126]



Last, the absence of obligation of notification is even less understandable in a situation where the further processing relates to individuals who are not suspects - but who can be witnesses or victims - in the context of a criminal investigation and even more in the absence of any suspects in the case of criminal surveillance.

[120] arts 12-20 GDPR.
[121] *Tele2 Sverige* (n 88).
[122] *Tele2 Sverige* (n 88) para 121.
[123] Such as national data retention law on communications data.
[124] See also Jasserand (n 29).
[125] Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data, 'practical guide on the use of personal data in the police sector', T-PD(2018)01, 15 February 2018.
[126] ibid 6.

## VI. Conclusions

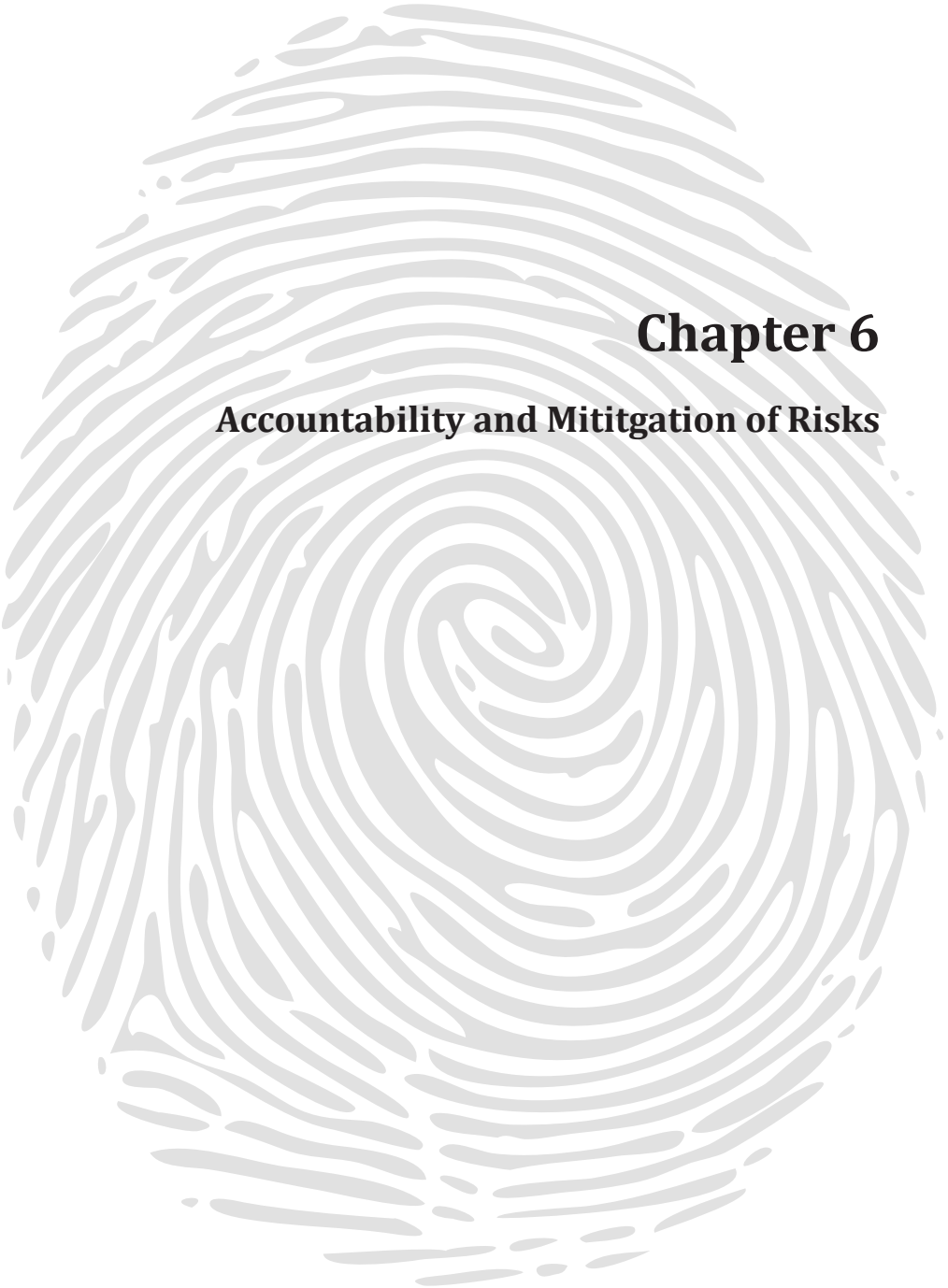
As demonstrated in this article and surprisingly, the principle of purpose limitation does not seem to play any role in the reprocessing of GDPR data for one of the purposes of Directive 2016/680. Still, the principle of purpose limitation is a constitutive element of the fundamental right to data protection.

First of all, if the GDPR and Directive 2016/680 define in identical terms the principle of purpose limitation, they do not provide similar rules concerning its application. In particular, Directive 2016/680 does not provide any guidance on the notion of 'compatible use', leaving the issue up to Member States. Instead, Directive 2016/680 provides, in Article 4(2), rules applicable to further processing. In the absence of precision, these rules seem to apply irrespective of the compatibility between the initial and secondary purposes of processing. As such, Article 4(2) of Directive 2016/680 can be construed as an exception to the principle of purpose limitation.

Second, the scope of the exception is not clearly defined. From the wording of Article 4(2) of Directive 2016/680, it is unclear whether it covers the further processing of personal data initially collected for a law enforcement purpose or the further processing of personal data initially collected for any purpose (which would include GDPR data).

Building on this textual ambiguity, the article has suggested two diverging paths: the application of Article 4(2) of Directive 2016/680 to the subsequent use of GDPR data or its exclusive application to 'police and criminal justice' data. In the first hypothesis, the principle of purpose limitation might play a role, which needs, however, to be redefined. In the second hypothesis, where the subsequent use of GDPR data most likely qualifies as initial processing under Directive 2016/680, the principle of purpose limitation does not play any role. That is problematic. First, Directive 2016/680 is a 'minimum harmonisation' Directive, leaving non-harmonised areas of Directive 2016/680 to the discretion of Member States. One could argue that the rules applicable to the further processing of GDPR data by law enforcement authorities are domestic issues. Second, like the United Kingdom and the Netherlands, Member States will most likely exclude the subsequent use of GDPR data for a law enforcement purpose from the scope of the provision implementing Article 4(2) of Directive 2016/680.

Ultimately, and contrary to the European Commission's views, not providing a specific legal basis for the further processing of GDPR data in a law enforcement context does not avoid 'creating problems'. The issue is thus left in the hands of Member States and their national courts until it gets challenged before the CJEU.



# Chapter 6

## Accountability and Mititgation of Risks

## *Chapter 6: Accountability and Mitigation of Risks*

*Through the Use of Data Protection Impact Assessment and Data Protection by Design and by Default Measures*

**Abstract:**
*The new data protection framework imposes an obligation of accountability to data controllers, who are responsible for the way they manage the personal data they process. Under this obligation, data controllers need to demonstrate their compliance with the data protection rules. Both the GDPR and Directive 2016/680 provide tools to 'implement' the accountability principle. Those tools are, in particular, the data protection by design and by default measures (DPbD) and the data protection impact assessment mechanism (DPIA). This chapter describes the tools and analyses how they could be used to protect the individuals' right to data protection in the scenario of re-use of GDPR biometric data for one of the law enforcement purposes covered by the 'police' Directive.*

### I. Introduction

The new data protection framework has introduced the principles of Data Protection by Design and by Default (DPbD)[1] and Data Protection Impact Assessment (DPIA) mechanism in the GDPR and the 'police' Directive.[2] These measures are part of the data controller's accountability and serve as safeguards to protect individuals' rights and freedoms (including the rights to data protection and privacy).[3] The term 'accountability' is mentioned in Article 5(2) GDPR describing the data protection principles applicable to the processing of data, and in recitals of both the GDPR and the 'police' Directive.[4] Although the term does not appear elsewhere, several authors have linked the obligation of accountability to Article 24 GDPR ('responsibility of the controller') and Article 19 of the 'police' Directive ('obligations of the controller').[5] Similarly worded in both instruments,[6]

[1] Recital 78 and art 25 GDPR, and Recital 53 and art 20 Directive 2016/680.
[2] Recital 84 and art 35 GDPR, as well as Recital 58 and art 27 Directive 2016/680.
[3] See in particular, EDPS, 'Opinion 05/2018, Preliminary Opinion on Privacy by Design' [2018], 8; and A29WP, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ' likely to result in a high risk ' for the purposes of Regulation 2016/679' [2017] WP248 rev.01, 4 [Guidelines on DPIAs].
[4] Recital 85 GDPR and Recital 61 Directive 2016/680.
[5] Even if the two articles do not mention the term 'accountability, the provisions are analysed as describing the content of the principle; see analysis by James X Dempsey, Fred H Cate, and Martin Abrams, 'Organizational Accountability, Government Use of Private-Sector Data, National Security, and Individual Privacy', ch 15 in Fred Cate and James X Dempsey (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data* (OUP 2017) 311.
[6] art 24(1) GDPR reads as follows: 'Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be

the principle requires data controllers to adopt *appropriate technical* and *organisational measures.* To do so, they must take into account the *nature, scope, context and purposes of processing* as well as the possible *risks* to data subjects' rights and freedoms. The principle of accountability is not a new concept, but it has been introduced as a new obligation in the data protection regulatory landscape.[7] It replaces the previous 'administrative burdens' imposed under the Data Protection Directive, and in particular the cumbersome notification to data protection authorities before processing personal data.[8]

The principle of accountability encompasses more than the principles of data protection by design and by default and data protection impact assessment. It also includes data security, data breach notification, the recording of processing activities as well as the logging obligation.[9] The purpose of this chapter is not to describe the different components of the principle of accountability, but to focus on the two key measures that are DPbD and DPIAs.[10]

Concerning data protection by design and data protection by default, the chapter does not discuss how to engineer the principles. This task is left to engineers and computer scientists. Technical experts have abundantly written on the engineering of Privacy by Design,[11] a close concept that has inspired the DPbD obligations.[12] Leaving the technical aspects of the concept aside, the chapter suggests some recommendations on data protection policies that should be adopted before law enforcement authorities can further

reviewed and updated where necessary.' The obligation is worded in similar terms in Art 19 Directive 2016/680, except that the obligation is addressed to Member States that should impose an obligation of accountability to data controllers in their national legislation in application of the Directive.

[7] For a detailed analysis of the principle of accountability under the GDPR, see Magdalena Brewczyńska, 'the Principle of Accountability in the General Data Protection Regulation: Calling the EU Legislator to Account for Limiting the Wording of Article 5(2) GDPR to Data Controllers' [2018] (LL.M thesis) <arno.uvt.nl/show.cgi?fid=144595> accessed 30 September 2018; see also EDPS, 'EDPS launches Accountability Initiative' [2016], factsheet <https://edps.europa.eu/sites/edp/files/publication/16-06-07_accountability_ factsheet_en.pdf> accessed 30 September 2018.

[8] See arts 18 and 19 Directive 95/46/EC, as well as the pre-GDPR area analysis of the A29WP in A29WP, 'Opinion 3/2010 on the principle of accountability' [2010] WP173, 15, and the Commission Staff Working Paper, Impact Assessment Accompanying the proposals for a Regulation and a Directive, SEC (2012) 72 final [2012], 79.

[9] See for instance, section 'Accountability and Governance' in ICO, 'Guide to the General Data Protection Regulation (GDPR)' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/> accessed 30 December 2018.

[10] The A29WP describes DPIAs as 'a key accountability tool' in A29WP, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' [2018] WP251 rev.01, 29; and the EDPS views 'privacy by design [as] an element of accountability' in EDPS, 'Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union' [2011], para 108.

[11] On engineering privacy by design, see for example ENISA 'Privacy and Data Protection by Design- from privacy to engineering' (Report 2014) <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> accessed on 30 September 2018; see also Seda Gürses, Carmela Troncoso and Claudia Diaz 'Engineering Privacy by Design' (2011), paper presented at the Computers, Privacy and Data Protection Conference; Jaap-Henk Hoepman, 'Privacy Design Strategies', Proceedings ICT Systems Security and Privacy Protection- 29th IFIP TC 11 International Information Security Conference (SEC 2014) <https://hal.inria.fr/hal-01370395/document> accessed on 30 September 2018.

[12] According to some scholars, for instance, Luiz Costa and Yves Poullet, 'Privacy and the Regulation of 2012' (2012) 28(3) Computer Law & Security Review 254, 260.

process biometric data originating from private parties. A part of the section on data protection by design and by default is based on a conference paper discussing the relationship between the concept of Privacy by Design and the principle of purpose limitation in the pre-GDPR area.[13]

Last but not least, since the literature on the topic in the field of law enforcement is still scarce[14] and the obligations are worded in similar terms in both instruments, this chapter builds on the analysis of the GDPR rules and their doctrinal interpretation.[15] However, ultimately, the recommendations are only provided for the reprocessing of biometric data in a law enforcement context.

Against this background, Section II analyses the principles of data protection by design and by default, while Section III focuses on the DPIA mechanism. Finally, Section IV offers some recommendations on the application of the measures to the subsequent use of GDPR biometric data by law enforcement authorities.

## II. Data Protection by Design and Data Protection by Default: Overarching Obligations

Data protection by design and data protection by default are two legal requirements introduced by Article 25 GDPR and Article 20 of Directive 2016/680. Data protection by design requires that data controllers implement technical and organisational measures to manage personal data and protect individuals' rights (including, but not limited to the right to data protection). The obligation must be implemented before and during the processing operations. Data protection by default is conceived as a separate obligation, which focuses on the implementation of the principle of data minimisation. This section explains the origin of the requirements through their link to the concept of Privacy by Design and discusses how data protection principles – in particular, the principle of purpose limitation- could be implemented before personal data are reprocessed for a law enforcement purpose.

[13] Catherine Jasserand, 'Legal Perspectives on the Difficult Relationship between the Concept of Privacy by Design and the Principle of Purpose Limitation at European Level' Conference Paper (Amsterdam Privacy Conference 2015).

[14] One should mention a Project Deliverable on DPIAs in the field of law enforcement, see Eva Schlehahn, Thomas Marquenie, and Els Kindt, 'Data Protection Impact Assessments (DPIAs) in the Law Enforcement Sector according to Directive (EU) 2016/680- A Comparative Analysis of Methodologies' (2016) Deliverable for the VALCRI project (Visual Analytics for Sense-Making in Criminal Intelligence Analysis) <http://valcri.org/our-content/uploads/2018/06/VALCRI-DPIA-Guidelines-Methodological-Comparison.pdf> accessed 30 December 2018; it should be observed that the methodologies reviewed are all based on the GDPR regime.

[15] The literature on GDPR provisions is already abundant; to name a few scholars, see for instance, Lina Jasmontaite et al, 'Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR' (2018) 4(2) EDPL 168; Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34(2) Computer Law and Security Review 279; Dariusz Kloza et al, 'Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework Towards a More Robust Protection of Individuals' (2017) d.pia.lab Policy Brief No. 1/2017 <https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf > accessed 30 September 2018.

## 1. Building on the Concept of Privacy by Design?

According to some authors,[16] data protection by design and data protection by design have been inspired by Privacy by Design. If the concepts are related, they are also distinct.

### *a. Privacy by Design*

There is not a single definition or approach to the concept of 'Privacy by Design.' Some authors have linked the notion to Privacy-Enhancing Technologies (PETs),[17] to the ethical concept of 'value-sensitive design'[18] - implying that human values should be taken into account in the design of technologies - or to Laurence Lessig's concept of 'code as law.'[19] The concept can thus take many forms and have different meanings. However, from a legal and policy perspective, one approach has dominated.

In the 90s, the former Information and Privacy Commissioner of Ontario, Ann Cavoukian, popularised the term and developed a policy concept around *7 foundational principles*.[20] The idea behind Privacy by Design is to take into account privacy issues - understood as issues relating to the management of personal data - from the design phase of a product, system, or service, to its deployment and use. Endorsed by data protection authorities at international level,[21] this approach was, however, harshly criticised for not being operational and implementable.[22] As analysed by Rubinstein and Good, Cavoukian published numerous papers on the application of Privacy by Design (including to biometric systems), but she did not translate the principles into an engineering approach.[23] To address this issue, several computer scientists suggested different strategies and methods engineering the concept.[24]

According to the European Network and Information Security Agency (ENISA), the meaning of the concept depends on its context of use. It refers to a 'general' principle in a legal context, while it means Privacy-Enhancing Technologies in a scientific context (such

[16] In particular, Costa and Poullet (n 12).
[17] See Enterprise Privacy Group, 'Privacy by Design: An Overview of Privacy Enhancing Technologies' (2008) <http://www.dsp.utoronto.ca/projects/surveillance/docs/pbd_pets_paper.pdf > accessed 30 December 2018.
[18] See in particular, the application of value sensitive design to technology design by Friedman in Batya Friedman, 'Value Sensitive Design' (1996) Interactions (November-December Issue).
[19] Lawrence Lessig, 'Code, Version 2.0' (Basic Books, 2006); on the origins of PbD, see Demetrius Klitou, 'The Value, Role and Challenges of Privacy by Design' ch 9 in *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century* (T.M.C Asser Press 2014).
[20] The 7 foundational principles are (1) Proactive not Reactive, Preventative not Remedial, (2) Privacy as the Default Setting, (3) Privacy Embedded into Design, (4) Full Functionality - Positive-Sum, not Zero-Sum, (5) End-to-End Security – Full Lifecycle Protection, (6) Visibility and Transparency-Keep it Open, and (7) Respect for User Privacy - Keep it User-Centric
<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> accessed 30 September 2018.
[21] 32nd International Conference of Data Protection and Privacy Commissioners, 'Resolution on Privacy by Design' Jerusalem, Israel, 27-29 October 2010 [2010] <https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf > accessed 30 September 2018.
[22] Gürses, Troncoso and Diaz (n 11); Ira Rubinstein and Nathaniel Good, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2013) 28 Berkeley Technology Law Journal 1133.
[23] Rubinstein and Good (n 20) 1338, fn 15.
[24] ibid; see also ENISA (n 11).

as computer sciences).[25] Regardless of its origin and exact meaning, the idea behind the concept is to 'build-in', 'integrate', 'embed' or 'incorporate' data protection or privacy principles in products, services, business practices and policies.[26]

In the EU data protection framework, the concept has not been introduced as 'Privacy by Design' but as 'Data Protection by Design and by Default.'[27] Beyond the terminology, there are differences between the two notions.

#### *b. The Concept in EU Data Protection Legislation*

Much before the formal introduction of the concept in the EU data protection framework, references to the notion could be found in Recital 46 and Article 17 of the Data Protection Directive.[28] Limited to security measures and IT systems, both provisions required data controllers to 'implement appropriate technical and organisational measures'[29] at the time of 'the design of the processing system and (…) of the processing itself.'[30]

The term 'Privacy by Design' is not used in the data protection framework, nor was it introduced in the legislative proposals of the new rules. The concept is replaced instead by the obligations of 'data protection by design' and 'data protection by default.'[31] Some authors consider the notions of 'Privacy by Design' and 'Data Protection by Design' as being synonymous,[32] whereas others distinguish them.[33] For instance, according to

[25] ENISA (n 11) 3-7.

[26] eg European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee of the Regions: A Comprehensive Approach to Personal Data Protection in the European Union' COM (2010) 609 final [2010] 12, n 30 where the Commission made a reference to its communication on PETs (COM (2007) 228) and stated that 'the principle of 'Privacy by Design' means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal' (emphasis added); see also Ann Cavoukian defining 'Privacy by Design' as 'an approach to protecting privacy by embedding it into the design specifications of information technologies, accountable business practices, and network infrastructures' in Ann Cavoukian, '*Privacy by Design* in Law, Policy and Practice, A White Paper for Regulators, Decision-Makers and Policy-Makers' (2011) 3
<http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf > accessed 30 November 2018.

[27] Title of both Art 25 GDPR and Art 20 Directive 2016/680.

[28] Peter Schaar, 'Privacy by Design' (2010) 2(3) Identity in the Information Society 267.

[29] art 17 (1) of the Data Protection Directive reads as follows:
'Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.'

[30] Recital 46 of the Data Protection Directive reads as follows:
'Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organisational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent unauthorised processing (…).'

[31] art 25 GDPR and art 20 Directive 2016/680.

[32] eg ENISA (n 11).

[33] Costa and Poullet (n 12) ask whether 'the change from PbD to Data Protection by Design [is] a specialization of meaning or [whether] the expressions [should] be considered as synonyms' (p. 260); Kung writes that 'Privacy-by-Design (PbD) focuses on requirements and measures that take into account the respect of individuals' privacy, while data protection by design focuses on requirements and measures to protect personal data' in Antonio Kung, 'PEARS: Privacy Enhancing Architectures' in Bart Preneel and Demosthenes Ikonomou (eds), *Privacy Technologies and Policies* (Springer 2014) 18; see also Jasmontaite et al (n 15) where the authors clearly distinguish the two concepts.

Hansen, the expression 'data protection by design and by default' has most likely been introduced in the new data protection rules to reflect the field of revision.[34] However, as explained in the next subsection, data protection by design (and by default) is not the mere implementation of the concept of Privacy by Design in the data protection field.

The principles of 'data protection by design' and 'data protection by default' are described in the GDPR and Directive 2016/680 as follows:[35]

> 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation [/Directive] and protect the rights of data subjects. ['Data Protection by Design']
>
> 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. ['Data Protection by Default']
> (…)

#### *c. Inspired by, but Different from, Privacy by Design*

Like Privacy by Design, data protection by design requires to take into account data protection principles from the conception of the design to the deployment and use of the services or products. As for data protection by default, the principle has been drafted as a separate obligation from data protection by design. This distinction constitutes a difference with the concept of Privacy by Design - as conceptualised by Cavoukian - where Privacy by Default is one of the elements of the concept. As analysed by Jasmontaite et al., in the EU data protection framework, *data protection by design* covers 'the design and existence of embedded safeguards and mechanisms' whereas *data protection by default*

[34] Marit Hansen, 'Data Protection by Default in Identity-Related Applications,' in Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell (eds), *Policies and Research in Identity Management* (Springer 2013) 4.
[35] art 25 GDPR and art 20 Directive 2016/680; the obligations in the Directive are addressed to Member States that must impose an obligation of data protection by design and by default to data controllers through their national legislation.

encompasses 'the implementation of such safeguards as a default setting.'[36] They are thus complementary.

Second, the material scope of data protection by design and data protection by default is more limited than that of Privacy by Design. The holistic principle of Privacy by Design - as approached by Cavoukian - applies to all the actors involved in the life cycle of the data: from the developers and manufacturers of systems or products to their vendors and end-users (i.e. the data controllers). By contrast, data protection by design (and by default) is limited to data controllers. Following Recital 78 GDPR, producers (of the products, services and applications) are only *encouraged* to take into account the right to data protection 'when developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task.' This *encouragement* is not legally binding. However, data controllers will most likely require producers and manufacturers to deliver products, services or apps that will enable them to comply with their data protection obligations.[37] The scope of the data protection by design and by default principles is more limited than what the Article 29 Working Party and the European Data Protection Supervisor had recommended: they both took the view that the principles should be binding on designers, producers, as well as on data controllers.[38]

### 2. Not all Data Protection Principles are Technically Embeddable

The aim of the principles of data protection by design and data protection by default is to ensure that data controllers adopt technical and organisational measures that implement data protection principles. However, neither the GDPR nor the new Directive expressly identifies data protection principles. Likewise, neither instrument explains what the 'technical and organisational measures' are, to the exception of anonymisation and pseudonymisation provided as examples of technical measures. Finally, in the proposal for the GDPR, the task of translating the principles into technical requirements was delegated to the European Commission,[39] but such a delegation disappeared in the final text adopted by the EU institutions.[40]

[36] Jasmontaite et al (n 15).
[37] Through contractual obligations; see also the analysis of Recital 78 GDPR by Bygrave in Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4(2) Oslo Law Review 105, 116-118.
[38] A29WP and the Working Party on Police and Justice, 'The Future of Privacy', Joint contribution to the Consultation of the European Commission on the legal framework to the fundamental right to protection of personal data, WP168 [2009], 13; A29WP, 'Opinion 8/2014 on Recent Developments on the Internet of Things' WP223 [2014]; EDPS, 'Opinion on the data protection reform package' [2012], 30.
[39] See art. 23(4) of the proposed General Data Protection Regulation read as followed: 'The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).'
[40] art 25 GDPR and art 20 Directive 2016/680.

### *a. Data Protection Principles*

Both Article 25 GDPR and Article 20 of Directive 2016/680 refer to 'data minimisation' as a data protection principle that should be implemented through organisational and technical measures. But they do not explain further what the other data protection principles are.

Neither the GDPR nor the 'police' Directive sets out a list of those principles.[41] They do list 'principles relating to the processing of personal data' in respectively Article 5(1) GDPR and Article 4(1) of the 'police' Directive, but the notion covers more than these principles. As a matter of example, the GDPR describes, in a non-exhaustive manner, what the notion encompasses in Article 47(2)(d) GDPR. This provision refers to the 'general data protection principles' as including the principles of 'purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies nor bound by the binding corporate rules.'[42]

There is thus some uncertainty concerning the principles that should be implemented in application of Article 25 GDPR and Article 20 of the Directive. But, since both provisions refer to data minimisation, it makes sense to consider, at least, that the principles applicable to the processing of personal data should be implemented by design and by default. That being said, data controllers should not limit themselves to these principles, as the notion of 'data protection principles' is rather broad. But, for the purpose of this chapter and because the research mainly focuses on the application of the principle of purpose limitation, the analysis only investigates the implementation of the principles described in Article 5(1) GDPR and Article 4(1) of the Directive.

### *b. Organisational and Technical Measures*

Both the GDPR and Directive 2016/680 formulate the obligations of data protection by design and by default as 'organisational and technical measures' that data controllers must adopt. But neither instrument defines these measures. They only refer to 'pseudonymisation' as one of the means to implement the obligations. It is argued that *technical measures* cover technical tools (such as anonymisation, pseudonymisation or data aggregation) that can implement data protection principles, whereas *operational measures* relate to procedures and policies that can be adopted to manage data processing. This chapter focuses on the latter, as the technical solutions should be elaborated in collaboration with technical experts. The distinction between organisational and technical measures is very useful since the paper claims that not all data protection principles –



[41] As a matter of comparison, it is interesting to note that the Council of Europe Convention 108 is more specific on the notion as it describes the 'basic principles for data protection' ie data quality that covers the rules applicable to data processing, data security, processing of special categories of data, and additional safeguards to data subjects (Chapter II of Convention 108).
[42] art 47(2)(d) GDPR, the list is non-exhaustive.

limited here to the principles relating to data processing- can be embedded into the design of technologies. Some principles, such as data minimisation or data security, are technologically implementable, whereas others such as the principle of purpose limitation have a policy component or require an assessment to be applicable. Thus, those principles can be implemented through policies or procedures, instead of technical solutions.

The classification of principles according to their ability to be 'technologically' implemented is inspired by the research made by two computer scientists. In *Engineering Privacy*, Sarah Spiekermann and Lorrie Cranor suggest a method to engineer the US Fair Practices Principles based on the distinction between notice and choice principles on one hand and data minimisation on their other hand.[43] They translate this distinction into a *privacy-by-policy* approach focusing on individuals' rights (such as information and consent) where individuals retain some control over their data and a *privacy-by-architecture* approach focusing on the architecture of IT systems (through data minimisation and data anonymisation).

Based on Spiekermann and Cranor's approach, this chapter argues that data protection principles can be divided into implementable and non-implementable principles. The first category covers data protection principles that can be built into a system or a product, such as data minimisation, data retention, or transparency.[44] The second category comprises principles that cannot be technologically implemented without first assessing their applicability or making a policy choice. It is the case of the principle of purpose limitation.[45]

#### *c. Principle of Purpose Limitation*

The principle of purpose limitation is laid down in Article 5(1)(b) GDPR and Article 4(1)(b) of Directive 2016/680. It is split between a principle of purpose specification and a prohibition of incompatible processing.[46] The first sub-principle describes the criteria that the purpose of data collection must meet, i.e. be 'specific', 'explicit' and 'legitimate'.[47] The second sub-principle relates to the prohibition of incompatible processing of personal data with the purpose(s) for which they were collected.[48]

It is argued here that, at the stage of the design of technologies and systems, not all (legal) subsequent uses of data can be foreseen. Some authors have suggested privacy design

[43] Sarah Spiekermann and Lorrie Faith Cranor, 'Engineering Privacy' (2009) 35(1) IEEE Transactions on Software Engineering 67.
[44] On data minimisation see, for instance, Gürses, Troncoso and Diaz (n 11); Spiekermann and Cranor (n 42), and Hoepman (n 11).
[45] For a detailed analysis of the principle of purpose limitation under both the GDPR and Directive 2016/680, see *Chapter 5* of this dissertation.
[46] See analysis by the A29WP on the components of the principle of purpose limitation in A29WP, 'Opinion 03/2013 on purpose limitation' [2013] WP2013, 11-13.
[47] art 5(1)(b) GDPR and art 4(1)(b) Directive 2016/680.
[48] ibid; see also the description of the 'block of compatible use' by the A29WP in A29WP, Opinion 3/2013 (n 43) 12-13.

strategies to implement the principle of purpose limitation into the design of IT products.[49] These strategies include, for instance, the unlinkability of databases containing personal data and the separation between processing and storage of personal data. However, to implement these strategies, one first needs to assess the legal ground on which the further processing can be carried out: it must be determined if the processing is based on the compatibility between the purposes of processing,[50] the existence of a specific law[51] or the individual's consent.[52] Thus the application of the principle of purpose limitation requires an assessment. Its interpretation is subject to changes to take into account the context or circumstances of the processing.

As analysed in previous chapters of this study,[53] the principle of purpose limitation is an essential principle that does not seem to play a significant role in the cases of subsequent uses of GDPR data for a law enforcement purpose. Should such processing follow the rules applicable to the further processing under 4(2) of the 'police' Directive? Or should such processing be considered as initial processing under the 'police' Directive?[54] Neither the 'police' Directive nor the GDPR covers the issue and thus answers the question. This issue might be then better addressed in data protection policies ('organisational measures') that describe the procedures to be followed in case the data originating from third parties (including private parties) are accessed for further use by law enforcement authorities.

As a suggestion, such a data protection policy could, at least, identify the following elements: (1) the legal ground(s) on which the access to and subsequent use of the data are allowed; (2) the source of the data (i.e. private sector); (3) the categorisation of data subjects (e.g. victims, suspects, witnesses, or third-party); (4) the classification of personal data (biometric data, including the type, such as fingerprints, facial images, voice samples, etc.); (5) the purpose(s) of law enforcement use(s) (such as criminal investigation, police-led surveillance); (6) the (number of) persons authorised to have access to the data; (7) the rules/procedures applicable to the management of the accessed data (such as their retention period, storage, etc.); (8) the rules/procedures applicable to (or prohibiting) any transfer of the accessed data (to other law enforcement authorities internally, within the EU, or outside the EU; to private parties, or to other public parties), and (9) the data subjects' rights (and in particular whether data subjects will be notified that their personal data have been transferred to and used by law enforcement authorities).[55]



[49] Hoepman (n 11) 7-9.
[50] In the context of GDPR processing, see art 6(4) GDPR.
[51] In the context of GDPR processing, see art 6(4) GDPR, and in the context of law enforcement processing, see art 4(2) Directive 2016/680.
[52] In the context of GDPR processing only, see art 6(4) GDPR.
[53] See *Chapters 4* and *5* of this dissertation.
[54] See, in particular, the analysis in *Chapter 5* of the dissertation.
[55] There is some uncertainty concerning the scope of the right to information in a law enforcement context, see previous *Chapters 4* and *5* of this dissertation.

Finally, the principles of data protection by design and by default are linked to the data protection impact assessment mechanism. The two types of measures are not exclusive of each other but complementary. As acknowledged in Recital 53 of Directive 2016/680, the results of a DPIA should be taken into account when developing specific data protection by design and by default solutions.

### III. DPIA: A Complementary Risk-Management Tool

Before the adoption of the data protection reform package, Privacy Impact Assessments (PIAs) were conducted voluntarily. The term 'data protection impact assessment' was not used.[56] In the UK, for instance, PIAs were part of 'best practices' under the Data Protection Act 1998 (implementing the previous Data Protection Directive)[57] and were also used by police authorities.[58] The novelty is their introduction in the new legal framework as a requirement triggered by the level of *risks* that data processing activities *are likely* to pose to individuals. As acknowledged by Kloza et al., the risk-based approach in the GDPR (as well as in the new Directive) originates from the field of risk management. In particular, "[t]he GDPR brought to the data protection fore terminology from risk management, such as 'high risk', 'likelihood', 'impact' or 'severity'".[59] It is thus difficult to define these terms with precision, and they might not be adapted to the legal fields of data protection and human rights.[60] According to the A29WP, this risk-based approach could already be found in Directive 95/46/EC, but was limited to 'security (Article 17) and [to] the DPA prior checking obligations (Article 20).'[61]

The DPIA requirement, formulated in Article 27(1) of Directive 2016/680, is described as follows:[62]

> Where a type of processing, in particular, using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of

[56] In the context of this paper, 'PIAs' and 'DPIAs' are used interchangeably; as it is often the case in other documents; see for instance, A29WP, Guidelines on DPIA (n 3) 4, fn 2.
[57] For example, Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR), Data Protection Impact Assessments (DPIAs)' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/> accessed on 30 December 2018.
[58] See, for instance, Nottinghamshire police, 'Privacy Impact Assessment (PIA)' [2012] (updated in 2013) <https://www.nottinghamshire.police.uk/sites/default/files/documents/files/PD608Privacy%20Impact%20Assessment%20v1%200.pdf> accessed 30 December 2018; North Wales Police, 'Body-Worn Video: Privacy Impact Assessment of Body Worn Video' [2014], updated in 2015 <https://www.north-wales.police.uk/media/427114/privacy-impact-assessment-body-worn-cameras.pdf> accessed 30 December 2018.
[59] Kloza et al (n 15).
[60] ibid.
[61] A29WP, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' [2014] WP218, 2.
[62] To be read together with Recital 58 Directive 2016/680.

the impact of the envisaged processing operations on the protection of personal data.[63]

As a result, only data processing operations that are 'likely to result in a high risk to the rights and freedoms of data subjects' lead to a DPIA. It must first be assessed when a processing operation triggers a DPIA before describing its content.

### 1. Initial Assessment: Risk Analysis

The key criterion is the level of risks posed by the processing operation(s) to individuals' rights and freedoms. A DPIA covers the right to data protection, as well as other rights and freedoms relating to data processing. These rights and freedoms are, among others, the right to information, the right to non-discrimination, the right to privacy, and freedom of expression.[64]

#### *a. High-Risk Processing*

'High risk' and 'risk' are not defined in the texts. Instead, the GDPR and Directive 2016/680 provide *factors* to determine the existence of high-risk processing. Those factors are the use of new technologies, as well as the nature, scope, context and purposes of the processing.

*i. Level of Risk*

According to Recital 52 of Directive 2016/680,[65] the level of risk should be assessed by reference to the likelihood of its occurrence and severity. The evaluation of the risk should result from an 'objective assessment.' However, the thresholds of 'severity', 'likelihood', and the notion of risk remain undefined. Likewise, neither instrument specifies what an 'objective assessment' is. In the law enforcement context, Recital 52 of Directive 2016/680 provides that *high risk* is 'a particular risk of prejudice to the rights and freedoms of data subjects.' Only in the context of GDPR data processing, does the Regulation identify three examples of 'high-risk' processing leading to a DPIA. Those cases are the systematic evaluation (including profiling) of individuals, the processing of sensitive data on a large scale, and the systematic monitoring of publicly accessible areas on a large scale.[66] The notion of 'large scale' is undefined as well. According to the A29WP, 'large scale' should be assessed thanks to the number of individuals affected by the processing, the type and volume of data, the duration of the processing as well as the geographical scope of the processing.[67]



[63] art 35(1) GDPR is worded in identical terms, to the exception that the Directive imposes an obligation on Member States to implement the rule.
[64] A29WP, 'Statement on the role of a risk-based approach in data protection legal frameworks' (n 57) 4, where the A29WP observed that "the scope of 'the rights and freedoms' of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion."
[65] and Recital 78 GDPR.
[66] art 35(3) GDPR.
[67] A29WP, Guidelines on DPIAs (n 3) 10.

The A29WP has established further guidance on the notion of 'high risk' in its Guidelines on DPIAs in the context of GDPR data processing. According to the Working Party, nine criteria can be used to evaluate whether a specific processing operation constitutes high-risk processing. A combination of two of these criteria is, at least, necessary to reach such a conclusion. These criteria are described as 1) evaluation or scoring; 2) automated decision making with legal or similar significant effect; 3) systematic monitoring; 4) sensitive data or data of a highly personal nature; 5) data processed on a large scale; 6) matching or combining datasets; 7) data concerning vulnerable data subjects; 8) innovative use or applying new technological or organisational solutions, and 9) processing that prevents data subjects from exercising a right or using a service or a contract.

In the UK, the Information Commissioner's Office (ICO) invites law enforcement authorities to follow the guidance it has developed for GDPR data processing. Its guidance refers to the criteria established by the A29WP. One could observe that some UK police authorities have already reproduced the ICO's guide on the GDPR in their data protection impact assessment policy.[68]

*ii. Objective Assessment, Likelihood, and Severity*

Several national DPAs have provided examples of DPIAs and explained the notion of 'objective assessment'. For instance, in the UK, the ICO suggests using a matrix combining both the severity and likelihood of risks to determine the level of risk. Following this approach, severity is split into 'serious harm', 'some impact', and 'minimal impact'; whereas the likelihood of harm is divided into 'remote', 'reasonable', and 'more likely than not.' For example, serious harm combined with a remote likelihood will result in low risk (and thus no DPIA), whereas serious harm will result in high risk if it is combined with a 'reasonable possibility' of harm or a 'more likely than not' harm.[69] In France, the CNIL (*Commission Nationale de l'Informatique et des Libertés*) scales the likelihood and severity of risks through a four-level typology: negligible risk, limited risk, significant risk, and maximum risk.[70] Thus different methodologies on the level of risks will apply at national level.[71]

[68] In particular, Dyfed Powys Police, 'Data Protection Impact Assessment Policy', 8 <https://www.dyfed-powys.police.uk/media/5874/data-protection-impact-assessment-policy.pdf > accessed 30 December 2018.

[69] For an overview of the matrix built by the ICO, see ICO's Guide 'Accountability and Governance: Data Protection Impact Assessments (DPIAs)' [2018] 33 <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf> accessed 30 September 2018.

[70] CNIL, 'Privacy Impact Assessment (PIA): Knowledge Bases' [2018] 4–5 <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf>accessed 30 September 2018.

[71] See also the other methodologies described in the VALCRI deliverable (n 14): The German 'Standard Data Protection Model' established by the German Data Protection Authorities (to the exception of Bavaria) <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf> accessed 30 December 2018; the DPIA Guidelines of the Belgium Data Protection Authority (*Commissie voor de Bescherming van de Persoonlijke Levenssfeer*) <https://www.gegevensbeschermingsautoriteit.be/aanbeveling-uit-eigen-beweging-mbt-de-gegevensbeschermingseffectbeoordeling-nr-012018> accessed 30 December 2018; the Spanish Data

*iii. Risk Leading to Potential Damage*

Neither the GDPR nor Directive 2016/680 requires the existence of actual damage, only possible harm to individuals, whether physical, material or non-material, is sufficient.[72]

***b. Factors***

The 'nature, scope, context and purposes of the processing' are factors that will also help establish the risky nature of a processing operation.[73]

In its Guidelines on DPIAs, the A29WP does not provide much guidance on these factors. At national level, the ICO offers more details on these factors.[74] The authority specifies that the *nature* of the processing relates to what the data controller 'plan[s] to do with the personal data.' It includes how the data are collected, stored, used, shared but also for how long they are kept, and how they are protected.[75] The *scope* of the processing is the core of the processing, in the sense that it covers the nature of the personal data at stake (including their sensitivity), the amount of data processed,[76] the number of data subjects, etc. The *context* of the processing provides 'the wider picture, including internal and external factors which might affect expectations and impact.'[77] Those factors are, for instance, the source of the data, the control that individuals can exercise over their personal data, but also the extent to which individuals expect the processing. Last, the *purpose* of the processing describes the reasons for the processing.[78] Its description should include the outcomes for individuals, but also the expected benefits for society at large as well as the existence of legitimate interests for processing on the data controller's side.[79]

The use of new technologies is another factor that should be taken into account in the assessment of the necessity of a DPIA. In its Guidelines on DPIAs, the A29WP gives the example of a technological solution that would use both 'fingerprint and face recognition' for access control.[80] As the use of such technology might 'involve new forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms,'[81] a DPIA might be necessary.


**2. Elements of a DPIA**

A DPIA results in mitigating the 'high risks' that have been identified. Thus, if data controllers conclude that they have to conduct a DPIA, they should provide solutions to mitigate, i.e. eliminate, minimise or reduce, the risks to data subjects' rights and freedoms.

Protection Authority (*Agencia española de protección de datos*<https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf> accessed 30 December 2018.
[72] Recital 75 GDPR and Recital 51 Directive 2016/680.
[73] A29WP, Guidelines on DPIAs (n 3) 17.
[74] ICO (n 56).
[75] ibid, see 'Step 2: How do we describe the processing?'
[76] ibid.
[77] ibid.
[78] ibid.
[79] ibid.
[80] A29WP, Guidelines on DPIAs (n 3) 10.
[81] ibid.

If a DPIA is mandatory, it should be carried out 'prior to the processing.'[82] As noted by the A29WP, a DPIA is not a static process, and it needs to be reviewed, updated and monitored.[83]

#### *a. Scope: Single Processing or a Series of Processing Operations?*

Following Recital 58 of Directive 2016/680, a data protection impact assessment in the context of law enforcement cannot relate to a single processing operation. It should, instead, cover 'systems and processes of processing operations.' This is different from the GDPR rules where a DPIA can relate to a single project.[84]

#### *b. Features of a DPIA*

According to Article 27(2) of Directive 2016/680,[85] a DPIA should, at least, contain the following elements:

a) a general description of the processing operations;
b) a risk assessment (including the identification of individuals' rights and freedoms that might be affected);
c) the mitigating solutions ('measures envisaged to address the risks'), and
d) safeguards, security measures and mechanisms for the protection of personal data.

Data controllers have a lot of flexibility concerning 'the precise structure and form of the DPIA.'[86] Several national data protection authorities have issued templates or examples of frameworks to guide data controllers. For example, the ICO has published a 'sample DPIA template' taking into account the GDPR provisions.[87] The process is composed of nine steps: from the identification of the need for a DPIA to the revision of the DPIA. In between, data controllers must identify the risks and find solutions to mitigate the risks. Thus, the preliminary assessment of the existence of 'high risk' processing can constitute a part of a DPIA. The CNIL has released a Privacy Impact Assessment template,[88] together with a methodology and a 'knowledge base' document.[89] However, they have not been specifically designed for law enforcement processing.

#### *c. Risk Mitigation*

The purpose of a DPIA is to identify solutions to minimise the risks to data subjects' rights and freedoms. As interpreted by the ICO, a mitigating measure should be envisaged for

[82] art 35(1) GDPR and art 27(1) Directive 2016/680.
[83] A29WP, Guidelines on DPIAs (n 3) 14.
[84] art 35(1) GDPR.
[85] See also art 35(2) GDPR.
[86] A29WP, Guidelines on DPIAs (n 3) 17.
[87] ICO, 'Sample DPIA Template' version v0.4 of 22 June 2018, downloadable from the section 'Data Protection Impact Assessments' in the Guide to the General Data Protection Regulation (n 56).
[88] CNIL, 'Privacy Impact Assessment (PIA): Templates' [2018] <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf> accessed 30 September 2018.
[89] CNIL, 'CNIL publishes an update of its PIA Guides' (*cnil.fr*, 26 February 2018) <https://www.cnil.fr/en/cnil-publishes-update-its-pia-guides> accessed 30 September 2018.

each risk identified.[90] There is no exhaustive list of solutions to address the risks. The measures have to be tailor-made to the risks identified, but they need to integrate data protection by design and by default solutions. They can vary from 'deciding not to collect certain types of personal data'[91] to 'anonymising or pseudonymising'[92] the data or 'making changes to privacy notices.'[93] In its DPIA template, the ICO advises to measure the effect of the solutions on the risk (risk eliminated, reduced or accepted) and the existence of residual risk (low, medium, high).[94]

If a residual 'high risk' has been identified, the national data protection authority needs to be consulted before the processing is carried out.[95] The data controller should provide the DPIA as conducted to the data protection authority.[96]

Based on the analysis of the provisions made in this section, the next section evaluates the level of risks associated with the law enforcement reprocessing of biometric data collected under the GDPR and provides some recommendations.

## IV. Law Enforcement Reprocessing of GDPR Biometric Data

In the scenario under review, personal data of a specific type - biometric data - initially collected under the GDPR are accessed and subsequently used for a law enforcement purpose. Such a scenario lies at the intersection between the GDPR and the 'police' Directive. The two instruments cover different fields, and some adjustments to the individuals' rights are necessary and justified in the context of law enforcement processing.[97] However, in that context like in the GDPR context,[98] the purpose of a DPIA is to assess the impact of the processing on individuals' rights. It seems, therefore, legitimate to investigate if and how the further processing of individuals' biometric data across fields impact their rights (including their right to remedy). Should the mere reprocessing of personal data across instruments not justify, on its own, a DPIA? Or should other elements be taken into account to assess the level of risk that such processing is likely to pose to individuals? Building on the findings of the previous sections, this part analyses different elements, which could be used to assess the necessity of a DPIA. It also offers suggestions on the content of such a DPIA.



[90] ICO (n 56)
[91] ICO (n 56) see 'Step 6: How do we identify mitigating measures?'
[92] ibid.
[93] ibid.
[94] ibid.
[95] art 36(1) GDPR and art 28(1)(a) Directive 2016/680.
[96] art 36(3)(e) GDPR and art 28(4) Directive 2016/680.
[97] Such as the need to not provide information about the data collected when a criminal investigation is ongoing.
[98] As observed by the A29WP in A29WP, Guidelines on DPIAs (n 3) 17, a DPIA is 'a tool for managing risks to the rights of data subjects, and thus takes their perspective.'

### 1. Preliminary Assessment

The criteria used in this section are based on those developed by the A29WP in the context of GDPR data processing; on the analysis made by the European Data Protection Board (EDPB) in its assessment of the draft lists submitted by national DPAs in application of Article 35(4) GDPR,[99] and on existing national data protection policies issued in the context of law enforcement.[100]

#### *a. Processing of Biometric Data: High-Risk Processing?*

In both instruments, the processing of biometric data is not classified, per se, as processing likely to result in a high risk to data subjects' rights and freedoms. But under certain conditions, such processing could be considered as high risk. For instance, under the GDPR, the processing of biometric data constitutes a high risk if the data are classified as sensitive (i.e. if they are processed to uniquely identify an individual)[101] and if they are processed on a large scale.[102] In the context of GDPR processing, the EDPB confirmed this interpretation in its opinions on the national draft lists of cases requiring a DPIA.[103] On the issue of biometric data processing, the Board clarified that the mere processing of biometric data is not sufficient to trigger a DPIA.[104] Instead, it considered that such processing is subject to a DPIA under two conditions: being carried out to uniquely identify an individual (i.e. being sensitive processing) and processed in conjunction with one of the criteria identified by the A29WP.[105]

In the absence of specific rules applicable to law enforcement processing, Member States and national DPAs are free to decide which processing operations fall within the category of 'high risk' processing. In the UK, the ICO has for instance extended the cases identified in the GDPR to law enforcement processing.[106] Concerning biometric data processing, some UK police authorities (e.g. the Dyfed Powys Police for example) have issued their

[99] art 35(4) GDPR provides the following:
'The supervisory authority shall establish and make public a list of the kind of processing operations for which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.'
[100] In particular, Dyfed Powys Police (n 65).
[101] According to art 9(1) GDPR and art 10 Directive 2016/680, the purpose of processing 'to uniquely identify an individual.'
[102] art 35 (3)(b) GDPR requesting a DPIA for the processing of sensitive data on a large scale.
[103] Under the consistency mechanism, the EDPB checks the consistent application of the GDPR rules throughout the EU, see art 64(1)(a) GDPR.
[104] Contrary to the position of nine DPAs (Croatia, France, Hungary, Ireland, Italy, Lithuania, Malta, Portugal, and the United Kingdom), see the Board's Opinions on their respective draft lists <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en> accessed 30 December 2018.
[105] See, for instance, EDPB, 'Opinion 22/2018 on the draft list of the competent supervisory authority of the United Kingdom regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)' [2018], 6 <https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion _2018_art._64_uk_dpia_list_en.pdf> accessed 30 December 2018.
[106] eg ICO, 'Data Protection Impact Assessments' under the section 'Law Enforcement Processing' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement processing/accountability-and-governance/data-protection-impact-assessments/> accessed 30 December 2018.

Data Protection Impact Assessment Policy where they list the processing of biometric data - without further condition - as triggering a DPIA.[107]

### *b. Types of Law Enforcement Purposes*

One could argue that the level of risk in a law enforcement context should be assessed according to the type of law enforcement purposes. For instance, the reprocessing of biometric data originating from the private sector might constitute a 'high risk' if it is carried out for criminal surveillance purposes because the surveillance might be untargeted or conducted in the absence of any offence or suspect. But, in the context of a criminal investigation that will identify a specific offence and one (or several) suspect(s), such a processing operation might not be 'high risk' processing in itself. The notion of 'high risk' needs thus to be tied to the impact that a specific processing operation would have on individuals. If in the context of a criminal investigation, police authorities request access to a privately–held biometric database, the request will most likely be targeted to one (or several) individual(s). By contrast, if police authorities would like to constitute a facial recognition database based on photographs held by social media and plan to use it for criminal surveillance purposes,[108] the impact on individuals will be higher.

### *c. Matching or Combining Different Datasets*[109]

According to the A29WP, matching or combining datasets is another criterion to take into account to evaluate the level of risk.[110] This criterion relates to the principle of purpose limitation and to the expectation that individuals might have regarding the further processing of their data. Indeed, when personal data collected for a specific purpose are reprocessed for a different purpose or by different data controllers, the new processing operation can entail risks to individuals' rights (in particular, individuals might not be informed about the secondary use of their personal data). Nuances should be added as, in the context of law enforcement processing, individuals do not have the same rights as in the GDPR context. However, if their data have been extracted from other datasets, they might not be aware of that processing. In the case of the reprocessing of GDPR data for a law enforcement purpose, this factor should also be tied to the origin or source of the data.

### *d. Data not Obtained Directly from Individuals*

The source of the data is not a criterion identified by the A29WP. In its opinions on national draft lists, the EDPB assessed the criterion of 'data collected via third parties' in the context of Article 19 GDPR. The element is not sufficient on its own and should be supplemented by another criterion to trigger a DPIA.[111] In the scenario under

[107] Dyfed Powys Police (n 65) 8.
[108] Assuming that such a database would be legal.
[109] This criterion established by the A29WP in its Guidelines on DPIAs (n 3) can be found in the Data Protection Impact Assessment Policy of the Dyfed Powys Police (n 65) 8.
[110] A29WP, Guidelines on DPIAs (n 3) 10.
[111] EDPB, 'Opinion 5/2018 on the draft list of the competent supervisory authority of Germany regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR) [2018], 7

consideration where personal data are reprocessed for a law enforcement purpose and accessed through private parties, this criterion is highly relevant.

#### *e. Exceptions to the Exercise of Individuals' Rights*

Besides, according to the EDPB, exceptions to individuals' rights (in particular, to the right to information) can constitute a factor to take into account together with another criterion.[112] In the context of law enforcement processing, data subjects' rights might also be subject to exceptions. These exceptions, restricting partially or completely their rights, might apply to the information given to them, to their right of access to the data, or their right of rectification or erasure.[113] It is suggested to extend the interpretation given by the EDPB to the context of law enforcement processing. As a consequence, a DPIA should be conducted and procedures put in place to deal with a situation where individuals are deprived of their rights when their biometric data are reprocessed, for instance, in the context of a criminal investigation.

#### *f. Use of New Technologies*

Following Article 27(1) of Directive 2016/680, the use of new technologies is also a factor to take into account to assess whether a specific processing operation might result in a high risk. This criterion is further explained in the A29WP Guidelines on DPIAs, and specific examples of such technologies are provided in the ICO's Guide on DPIAs. Among others, techniques that involve machine learning or artificial intelligence to collect or analyse personal data are considered as innovative technologies.[114] According to the EDPB, the use of new technologies is not sufficient in itself to constitute a high risk. It needs to be in conjunction with another criterion to be classified as 'likely to result in a high risk.'[115] In the field of law enforcement, one could think of the use of big data analytics to extract information about (potential) suspects.[116] The risks to individuals' rights could

<https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52018-germany-sas-dpia-list_en> accessed 30 December 2018.

[112] See for instance EDPB, 'Opinion 16/2018 on the draft list of the competent supervisory authority of the Netherlands regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR)' [2018], 7 where the EDPB states that 'a processing activity conducted by the controller under Article 14 GDPR and where the information to be given to the data subjects is subject to an exemption under Article 14.5 (b)-(d) could require a DPIA to be carried out only in conjunction with at least one other criterion'
<https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_nl_sas_dpia_list_en.pdf> accessed 30 December 2018.

[113] Respectively art 13(3), art 15 (1), and art 16(4) Directive 2016/680.

[114] ICO, Data Protection Impact Assessments (n 56), 'Examples of processing likely to result in high risk'
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/> accessed 30 December 2018.

[115] eg EDPB, 'Opinion 13/2018 on the draft list of the competent supervisory authority of Lithuania regarding the processing operations subject to the requirements of a data protection impact assessment (Article 35.4 GDPR) [2018], 8
<https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_lt_sas_dpia_list_en.pdf > accessed 30 December 2018.

[116] On the use of big data analytics by law enforcement authorities, see, for instance, Sarah Brinkhoff, 'Big Data Data Mining by the Dutch Police: Criteria for a Future Method of Investigation' (2017) 2(1) European Journal for Security Research 57.

be heightened when the data are mined from social media for criminal surveillance purposes.

Following the analysis made in this subsection, the reprocessing of GDPR personal data for a law enforcement purpose is not listed as a type of processing operations requiring a DPIA. However, it meets enough criteria to trigger a DPIA. For instance, it relates to the processing of sensitive data, which were not obtained from the data subject. It might also combine data from other sources and involve new technologies.

### 2. Elements of the DPIA

Directive 2016/680 does not impose any methodology or form to conduct a DPIA. Following Recital 58 of the Directive, a DPIA should, however, contain certain features and be limited to 'relevant systems and processes of processing operations.'[117] Thus a DPIA in the context of law enforcement does not cover a single processing operation. It is therefore recommended that law enforcement authorities adopt procedures (or a data protection policy) addressing the further processing of personal data (including sensitive data) held by private parties and collected under the GDPR. Such a policy should refer to the elements outlined below.

#### *a. Description of the Processing*

According to Article 27(2) of Directive 2016/680, the data controller should describe the nature, scope, context and purposes of the intended processing operations. Concerning the *nature*, the data controller should mention the source of the data (private parties), how the data will be further used (for surveillance purposes or in the context of a criminal investigation), who will have access to the data (including a limited number of individuals allowed to access the data), how the data will be secured, for how long the data will be kept and whether they will be combined with other data or used for a different purpose.

The scope of the processing should mention the nature and sensitivity of the data, which are two critical factors. In the scenario under review, biometric data fall within the category of sensitive data if they are processed to uniquely identify an individual or if they reveal sensitive data.[118] The status of individuals concerned by the processing is also essential: whether they are suspects, witnesses, victims or third parties.

Concerning the *context* of the processing, one of the relevant factors is the control that individuals can exercise on their data. The source of the data is also highly relevant.

Concerning the *purpose* of the processing, the further processing of the data for a criminal investigation purpose will not have the same impact on individuals' rights and freedoms as the same processing in the context of criminal surveillance. In the first case, it would be

[117] Recital 58 Directive 2016/680.
[118] art 10 Directive 2016/680.

highly relevant to know the status of the individuals concerned by the processing (suspects or not). In the second case, it would be essential to know whether an individual is suspected or whether the surveillance is untargeted (with the risk of profiling individuals).

***b. Risks***

No list of risks can be established as the assessment depends on the type of law enforcement purpose as well as on the status of individuals involved (suspects, non-suspects, witnesses, victims). However, the following risks could, at least, be identified: the risks associated with the collection and use of the data, as well as the risks that relate to the security, storage and retention of the data.

The risks related to the reprocessing of personal data originating from a different source are, for instance, the risks of unauthorised access, use or disclosure of the data (e.g. by unauthorised staff). Since the data were initially collected for a different purpose, there is also a risk of inaccuracy of the data. The reprocessing might also entail risks linked to the retention and storage of accessed data. Finally, if the data are reprocessed using innovative technologies (to mine social media for example), such reprocessing might impact the right to privacy.

***c. Safeguards and Solutions***

An assessment of the necessity and proportionality of the processing should be performed. For each risk identified, a solution should be proposed. In the case of the reprocessing of GDPR biometric data for a law enforcement purpose, the following measures could be considered: 1) identifying the legal basis to request access to the data (including the existence of a data-sharing agreement); 2) defining a clear scope of processing (e.g. access to the data concerning a specific individual in the context of a criminal investigation); 3) limiting the processing to the data strictly necessary to the law enforcement purpose identified; 4) securing the data collected; 5) defining the period of retention (depending as well on the status of the individuals impacted by the processing); 6) not linking the data to other cases that are not covered by the purpose of processing; 7) describing clear data protection procedures to follow before reprocessing sensitive data originating from the private sector, and 8) drafting a procedure to inform individuals about the processing as soon as such a notification can no longer prejudice the purpose for which the data were processed. On this last measure, one should note the discussion on the scope of the right to information as drafted in Directive 2016/680. It is uncertain whether Article 13 of the Directive obliges Member States to impose a duty of notification to data controllers who reprocess personal data collected for a different purpose (including a GDPR purpose). But nothing prevents law enforcement authorities from adopting procedures to inform individuals about the (re)processing of their biometric data in a law enforcement context.

As rightly observed by the ICO, the list of mitigating measures cannot be exhaustive as it needs to be adjusted to the specificities of the processing operations. However, data controllers should review their procedures (to keep them up to date) and document the processing operations.[119]

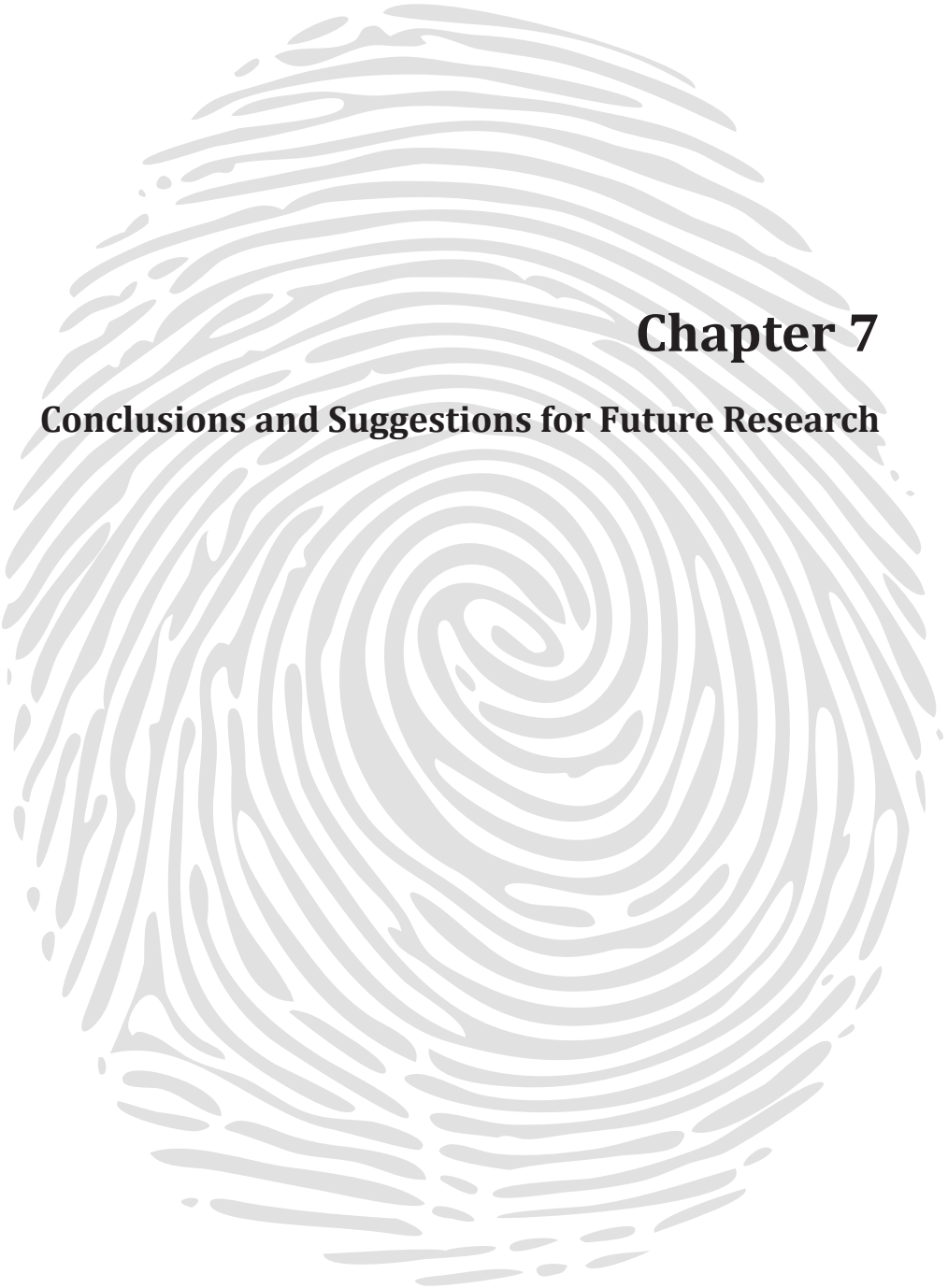
Last, but not least, the procedures put in place should also reflect data protection by design and by default measures. In particular, the description of a DPIA should describe the technical solutions adopted regarding data retention, data minimisation and data storage. The procedures adopted to manage the risks to data subjects' rights and freedoms are also part of data protection by design (and by default) measures that data controllers must implement.

## V. Conclusions

The GDPR and the 'police' Directive have set out two essential accountability tools: the Data Protection by Design and by Default obligations and the Data Protection Impact Assessment measures. However, both instruments remain vague about the implementation of these tools. Data protection by design and data protection by default are overarching obligations encompassing procedural and technological solutions. Focusing on the procedural aspect of DPbD and more specifically on the implementation of the principle of purpose limitation, the chapter suggests the adoption of a data protection policy to handle the case of the reprocessing of personal data across instruments.

As for Data Protection Impact Assessment, it is conceived as a complementary tool that follows a risk-based approach. It only becomes mandatory where data processing is 'likely to result in a high risk' to individuals' rights and freedoms. 'High risk' is thus the key notion to trigger a DPIA. Undefined in both the GDPR and the 'police' Directive, the notion has been clarified by the A29WP and several national DPAs. However, their guidance is not specific to law enforcement processing and does not take into account the case of the reprocessing of personal data across fields. Building on the criteria established by the A29WP, while acknowledging the specificities of the field of law enforcement, this chapter suggests an interpretation to assess the risks posed by the reprocessing of biometric data for a law enforcement purpose. It argues that the further processing of sensitive data collected under the GDPR meets enough criteria to conclude that a DPIA should be conducted. However, what is missing is the acknowledgement that such law enforcement processing of sensitive data collected for a GDPR purpose triggers on its own a DPIA. A clarification on this issue by the EDPB would be welcome as the Board has the power to 'oversee the implementation of the Data Protection Law Enforcement.'[120]


[119] See Recital 56 and art 24 Directive 2016/680.
[120] EDPB, 'Europe's new data protection rules and the EDPB: giving individuals greater control' (press release, 25 May 2018) <https://edpb.europa.eu/news/news/2018/europes-new-data-protection-rules-and-edpb-giving-individuals-greater-control_en > accessed 30 December 2018.



# Chapter 7

## Conclusions and Suggestions for Future Research

## *Chapter 7: Conclusions and Suggestions for Future Research*

The research aimed to establish whether the new EU data protection framework provides adequate safeguards to individuals, whose biometric data collected under the GDPR are reprocessed for one of the 'police' Directive purposes. To answer the research question, the study investigated three issues. It first analysed the legal regime applicable to the notion of biometric data introduced as a category of personal data in the new legal framework. It also deconstructed the concept from a technological perspective to understand the impact of the statutory definition on the technical processing of biometric data. The research then analysed the interface between the GDPR and the 'police' Directive to determine the existence of safeguards. By doing so, it discussed the role of the principle of purpose limitation and assessed the safeguards provided by the 'police' Directive (such as the right to information) based on the ECJ case law on data retention. Finally, in an attempt to provide recommendations, the research analysed new tools introduced in the EU data protection framework, namely the Data Protection Impact Assessment and the Data Protection by Design and Default principles. In the search for the individuals' safeguards, the study has uncovered important findings and reached significant conclusions.

**First, the unsettled meaning of biometric data from a data protection perspective creates legal uncertainty.** What seemed to be a *terminological* discussion on the notion of 'biometric data' at the start of the study became a crucial debate on the scope of the notion as the research progressed. As explained in *Chapter 2*, 'biometric data' was not legally defined in the EU data protection landscape until its introduction in the new legal framework. However, as analysed in *Chapter 3*, the statutory definition is imprecise and disconnected from its scientific meaning. It is indeed difficult to grasp what the legal notion encompasses. The definition does not accurately refer to the verification and identification modalities for which biometric data are processed to perform biometric recognition. It refers instead to the enigmatic phrases of 'allowing the unique identification' and 'confirming the unique identification.'

More confusion is brought by Recital 51 GDPR, which is supposed to clarify when photographs are covered by the definition of biometric data. The recital refers to their technical processing that 'allows unique identification' or 'authentication'. Used in opposition to 'authentication',[1] *unique identification* is understood as referring to the identification modality. However, this reading is not consistent with the definition of

[1] Authentication and verification are commonly used as synonyms, even if the biometric community recommends that the term 'verification' be used exclusively; see ISO/IEC Standard 2382-37 on the harmonisation of biometric vocabulary, term 37.01.03, note 6.

biometric data in Article 4(14) GDPR where the modalities are described as 'allowing the unique identification' and 'confirming the unique identification.' To date, the literature on this issue is scarce but shows the discrepancy existing between the article and the recital.[2] In the law enforcement context, there is not such a discussion since Recital 51 has no equivalent in the 'police' Directive. The notion of biometric data described in Article 3(14) of the Directive is worded in the same terms as Article 4(14) GDPR. That being said, the 'police' Directive does not offer any clue on the meaning of *unique identification*.

This dissertation takes the view that *unique identification* does not refer to a specific recognition modality. It should, instead, be understood as a threshold of 'identification' from a data protection perspective. Identifying an individual in a data protection context does not mean establishing his or her civil identity. It means singling out an individual, distinguishing him or her from a group of people.[3] As for the meaning of *unique identification*, this research has built on the interpretation used in the doctrine of the notion of 'personal data' under the Data Protection Directive of 1995. In particular, Kostchy has interpreted *unique identification* as being the 'highest degree of identification' that could be achieved through unique features, such as biometric data.[4] In that case, the identification is 'unique' because the characteristics that are used to identify someone (i.e. to single out) are deemed unique to that individual.[5] Following this interpretation, identification based on biometric data is 'unique' whether the data are processed for biometric identification or verification purposes. In both cases, the individual is *singled out* thanks to his or her biometric data.

It is crucial to determine the meaning of *unique identification* since it is also used as the criterion for classifying biometric data into the category of sensitive data. Following Article 9(1) GDPR and Article 10 of the 'police' Directive, only the biometric data that are processed to 'uniquely identify' an individual are sensitive data.[6] It is therefore necessary to know whether biometric data processed for both identification and verification purposes fall within that category. The rules applicable to the processing of sensitive data are indeed more stringent than the rules applicable to the processing of ordinary personal data. The biometric community and the many companies that offer biometric solutions for verification purposes need to know whether these operations are sensitive or not. In this dissertation, it has been argued that biometric data processed for both types of purposes



[2] See Catherine Jasserand, 'Legal Nature of Biometric Data: from 'Generic' Personal Data to Sensitive Data' (2016) 2(3) EDPL (see *Chapter 3* of the dissertation) and Els Kindt, 'Having Yes, Using No? About the New Legal Regime for Biometric Data' (2018) 3(2) Computer Law & Security Review 433.
[3] As defined in A29WP, 'Opinion 4/2007 on the concept of personal data' WP136 [2007] 13.
[4] Waltraut Kotschy, 'Article 2, Directive 95/46/EC' in Alfred Büllesbach, Serge Gijrath, Yves Poullet and Corien Prins (eds), *Concise of European IT law* (2nd edn, Kluwer Law International 2010), 35; see also analysis by the A29WP in A29WP, Opinion 4/2007 (n 3) 8-9.
[5] One could dispute the alleged 'uniqueness' of biometric characteristics and refer instead to their distinctiveness, as discussed in *Chapter 2*.
[6] Biometric data that reveal sensitive information (such as political opinions, religious beliefs, or health conditions) could still be considered sensitive data but not because they are biometric data.

are sensitive data. However, in the absence of a binding decision or interpretation on that definition, the uncertainty for users, data controllers and data subjects remains.

Finally, one could regret that the statutory definition was not crafted in collaboration with the biometric community. The definition could have referred to the wording used in the technical definitions instead of using ambiguous terms.[7] In other countries, such as Australia, the national law on data privacy makes an explicit reference to the identification and verification purposes for which biometric data are used. For instance, the definition of sensitive information includes 'biometric information that is used for the purpose of automated verification or biometric identification.'[8] Such a clarification would have avoided speculation on the types of biometric data that fall into the category of sensitive data. In the end, if it is true that the legislation should remain technology-neutral, it should however not regulate technological fields without understanding the impact that the rules will have on these fields.

**Second, the analysis of the interface between the GDPR and the 'police' Directive shows no specific role played by the principle of purpose limitation in a scenario where personal data are first collected under the GDPR and further processed by law enforcement authorities for one of the purposes of the 'police' Directive.** Before the adoption of the 'police' Directive, the framework applicable to the processing of personal data for law enforcement purposes was fragmented. The cross-border processing of personal data was regulated by the Council Framework Decision 2008/977/JHA, whereas the processing of personal data at domestic level was left to the discretion of Member States who could follow the non-binding Recommendation R(87)15 of the Council of Europe on the use of personal data in the police sector.[9]

With the adoption of the 'police' Directive, the same rules apply to the domestic and cross-border data processing operations for law enforcement purposes. However, the processing operations of personal data for law enforcement and non-law enforcement purposes remain split between the 'police' Directive and the GDPR. This split of rules justified assessing the impact that a possible discrepancy between the instruments could have on the protection granted to individuals. It was also assumed that the implementation of the 'police' Directive into national law could further increase the risk of discrepancy among Member States. The interface between the GDPR and the 'police' Directive became thus an essential issue of the study, raising the question of the role

[7] Using for instance, the definition provided in the ISO/IEC Standard 2382-37 on the Harmonisation of Biometric Vocabulary, as suggested in *Chapter 2* of the dissertation.
[8] Australian Government- Federal Register of Legislation, *Privacy Act 1998*, Section 6(1) <https://www.legislation.gov.au/Details/C2014C00076> accessed 30 November 2018.
[9] Despite its non-binding nature, the Recommendation has been used as a 'data protection standard' in different instruments including the Europol Regulation (Regulation 2016/674); on this issue see Mireille Caruana, 'The Reform of the EU Data Protection Framework in the Context of Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement' (2017) International Review of Law, Computers & Technology 1, 3.

played by the principle of purpose limitation in the scenario of law enforcement use of biometric data collected by private parties.

As established in *Chapter 4* and *Chapter 5*, both instruments delimit their application through the reference to each other's scope and define the rules applicable to the further processing. The GDPR establishes the rules for the further processing of personal data collected for a GDPR purpose, while the 'police' Directive provides the rules applicable to personal data collected and further processed for a law enforcement purpose. However, uncertainty remains concerning the rules applicable to processing operations across the two instruments. Moreover, the question is whether the subsequent use of GDPR data is an initial processing operation or a further processing operation under the 'police' Directive. In this specific scenario introduced in *Chapter 4* and thoroughly analysed in *Chapter 5*, the principle of purpose limitation seems to have been forgotten.

The absence of a clear role for the principle of purpose limitation is problematic for at least two reasons. First, the principle is part of the fundamental right to data protection enshrined in Article 8 of the Charter. As such, it should constitute a guarantee for the protection of individuals' personal data. Second, its purpose is to frame the conditions for subsequent processing of personal data. Derogations and exceptions to the principle are possible; however, the processing needs to comply with specific conditions (either individual's consent or a legal obligation to safeguard compelling interests under the GDPR, or a legal basis combined with the principles of proportionality and necessity under the 'police' Directive).[10] As resulting from the detailed analysis of *Chapter 5*, the scenario has not been clearly established, nor clarified in any recital. It even seems that the case was purposely avoided,[11] leaving Member States free to decide how they would consider the reprocessing of GDPR personal data under the 'police' Directive rules. This situation reveals a gap between the two instruments and highlights the difficulty raised by the split of rules between two distinct instruments.

As a matter of comparison, the practical guide on the police use of personal data, issued by the Council of Europe Consultative Committee of Convention 108, provides guidance on a similar scenario.[12] The guide contains a specific section on the access to and use of data held by private parties. It identifies two cases where police authorities may access data collected for a different purpose: in relation to 'an on-going investigation' or 'to identify thematic trends in relation to a certain type of crime.' The guide also makes an express reference to the principle of purpose limitation when it clarifies that such access and use



[10] art 6(4) GDPR and art 4(2) Directive 2016/680, respectively.
[11] See the discussions in *Chapter 5* of the dissertation, under Section III entitled 'Regime of Purpose Limitation under Directive 2016/680'.
[12] Council of Europe, Consultative Committee of Convention 108, 'Practical Guide on the use of personal data in the police sector', T-PD (2018) 01 [2018].

need to be 'authorised or be underpinned by a legal obligation to comply with the purpose limitation principle.'[13]

As concluded in *Chapter 5*, the absence of clear rules on further processing across the two instruments does not avoid 'creating problems.'[14] It only offloads the issue on to Member States, leading potentially to a greater discrepancy.

**Third, the testing of the 'police' Directive provisions against the ECJ's benchmark on data retention has revealed shortcomings of the Directive (in particular, in the formulation of the right to information).** To assess whether the provisions of the 'police' Directive provide adequate safeguards to individuals whose personal data are accessed for re-use by law enforcement authorities, the study searched for a benchmark to test these provisions. The Court of Justice has not yet delivered any judgment on an identical scenario but it has on the close scenario of data retention, where personal data collected by private parties are kept following a legal obligation to allow law enforcement authorities to access and re-use the data.[15] The difference between the two scenarios thus lies in the obligation to retain the data. As the ECJ clearly distinguished the issue of retention from that of access and re-use in its case law, the research analysed the Court's findings on this second aspect.

Keeping in mind these differences, *Chapter 4* tested the provisions of the 'police' Directive against the standards of *Digital Rights Ireland* and *Tele2 Sverige.* Building on the opinions of the European Parliament and the European Commission,[16] it was argued that the findings of the case law should apply beyond the field of data retention, and in particular to cases where personal data held by private parties are accessed and used by law enforcement authorities. The analysis further revealed that the 'police' Directive might fall short on several accounts. In particular, the Directive does not provide objective criteria to define the conditions under which law enforcement authorities could access and further use personal data generated by private parties for a different purpose. Besides, it lacks a specific procedural rule on the prior review of a request for access,[17] and the right to information in Article 13 of the Directive is not expressly formulated as a right of notification. On this last issue, the Court held in its case law that individuals whose data

[13] ibid 14.
[14] In reference to the European Commission's position during the negotiations of the draft police Directive at the Council level, where the Commission justified the absence of specific rules in the draft Directive based on the fact that "the further processing across the two legal instruments would create problems", see *Chapter 5*, footnote 49.
[15] See Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* [2014] ECLI:EU:C:2014:238, and Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and others* [2016] ECLI:EU:C:2016:970.
[16] See *Chapter 4,* Section III entitled 'Existence of Substantive and Procedural' Safeguards in Directive 2016/680?'
[17] On this latter it could be argued that not every reprocessing operation for a law enforcement purpose would require prior review, but only the ones that have serious consequences on individuals, such as situations where there is no offence or suspect (eg in cases of criminal surveillance).

have been accessed by law enforcement authorities should be notified at a given point in time, i.e. at least at a time when the investigation can no longer be prejudiced.[18] The notification triggers their right to remedy as well as other rights (such as the right of access, and rectification). Yet the Directive does not oblige Member States to introduce in their national law an obligation to notify the processing, and a fortiori, the further processing of the data.

The right to information is formulated in Article 13 (1) of the Directive as a right to 'make available information' to individuals, which raises the question of whether individuals need to have prior knowledge about the processing operation to exercise their right to information and the other rights deriving from it. This obligation is completed by Article 13(2) that stipulates that Member States should impose on data controllers an obligation to 'provide…in specific cases…further information' to enable individuals to exercise their rights. These cases –which do not seem to be entirely defined – include the situation where data have been collected without the knowledge of individuals.[19] For some authors, this provision is the evidence that the obligation of notification is included in the Directive.[20] However, nowhere in the 'police' Directive is there any express mention of the obligation to *notify* individuals, nor of a time when the notification should be made. In the end, based on this ill-defined provision, Member States are not compelled to impose an obligation of notification to the law enforcement authorities.

The obligation of notification derives from the judgment in *Tele2 Sverige*, which was handed down after the adoption of the 'police' Directive. Hence, the Directive could not have reflected this finding in its provisions. However, the ECtHR set up earlier the obligation of notification in its case law on the interpretation of Article 8 ECHR in criminal surveillance cases.[21] As such, the obligation should have been reflected – and in specific terms – in the 'police' Directive. The research suggests that the right to information should be interpreted in light of the ECJ and ECtHR case law to allow individuals to be informed and exercise their rights.

Last, a distinction should be made between the obligation of transparency and the obligation of notification. Being transparent about the way personal data are processed in general is different from informing an individual about a specific processing operation. The 'police' Directive mentions in a recital that processing should be transparent but has

[18] *Tele2 Sverige* (n 15) para 121.
[19] art 13(2)(d) Directive 2016/680 reads as follows: '[…Member States shall provide by law for the controller to give to the data subject, in specific cases, the following further information…](d) when necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.'
[20] See Paul de Hert and Juraj Sajfert, 'Police, Privacy and Data Protection from a Comparative Legal Perspective' in Monica den Boer (ed) *Comparing Policing from a Legal Perspective* (Edward Edgar 2018), 321; however, the authors only state that 13(2)(d) Directive 2016/680 encompasses the obligation of notification without explaining their reasoning.
[21] See *Klass and others v Germany* App no 5029/71 (ECHR, 6 September 1978), para 57 et seq; *Weber and Saravia v Germany* App no 54934/00 (ECHR, 29 June 2006), para 135; *Roman Zakharov v Russia* App no 47143/06 (ECHR, 4 December 2015), para 287 et seq; see also the analysis in Paul de Hert and Franziska Boehm, 'The Rights of Notification after Surveillance is over' (2012) Digital Enlightenment Yearbook 19.

not conveyed this obligation in any of its provisions.[22] As a consequence, law enforcement authorities are not required to explain how personal data personal data can be (re-) processed.[23] On this issue, one should observe that the practical guide on the police use of personal data, illustrating the application of Recommendation R(87)15, is more specific. It distinguishes *general* information from *specific* information, which must be both provided to individuals. General information corresponds to the obligation of transparency, whereas specific information is the information given to an individual about specific processing operations. Concerning specific information, the guide stipulates that in case a restriction or derogation applies, the information should be provided to an individual 'as soon as it no longer jeopardises the purpose for which the data were used.'[24] This condition echoes the findings of the ECJ in *Tele2 Sverige*.[25] Alternatively, it could be that *Tele2 Sverige* implicitly refers to the ECtHR jurisprudence on criminal surveillance.[26]

**Fourth, the accountability tools of Data Protection by Design and Default as well as Data Protection Impact Assessment might help to mitigate the risks to the individuals.** Both measures have been introduced in the new EU data protection framework to support the accountability of data controllers. As suggested in the analysis of *Chapter 6*, they can also be used as extra safeguards for individuals whose personal data are reprocessed for a law enforcement purpose. But neither the GDPR nor the 'police' Directive offers specific guidance on their application. Data Protection by Design and Default is an overarching principle that can cover both data protection policies and privacy-preserving solutions (such as encryption of the data, anonymisation of the data). As technical solutions are left in the hands of technical experts, the dissertation has only identified elements to be included in data protection policies to enable law enforcement authorities to reprocess biometric data originating from private parties.

Data Protection Impact Assessment is a complementary tool to Data Protection by Design and Default. It is not systematically carried out as not every processing operation is subject to a DPIA. Only the ones that are 'likely to result in a high risk' to individuals' rights and freedoms require a DPIA. On what constitutes such a high risk, the GDPR is more detailed than the 'police' Directive. Thus, the DPIA framework set under the GDPR is used

[22] Recital 26 of Directive 2016/680 provides that 'any processing of personal data must be lawful, fair and transparent…'
[23] Compare art 4(1)(a) Directive 2016/680 (personal data should be 'processed lawfully and fairly') with art 5(1)(a) GDPR (personal data should be 'processed lawfully, fairly and in a transparent manner in relation to the data subjects'); also compare art 12 GDPR on data subjects' right with art 12 Directive 2016/680 where the adjective 'transparent' does not appear in the communication form of the information. On the absence of the principle of transparency, see also analysis by the European Union Agency for Fundamental Rights, 'Handbook on European Data Protection Law' (2018) 283.
[24] ibid.
[25] *Tele 2 Sverige* (n15) para 121: '…the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer able to jeopardise the investigations being undertaken by those authorities.'
[26] Para 121 of *Tele2 Sverige* (n 15) describes the obligation of notification without referring to the ECtHR case law but the wording used to describe the obligation is close to that of the ECtHR in criminal surveillance cases (n 21).

as guidance for the regime applicable in the law enforcement context. In particular, 'any type of biometric data processing' on its own is not sufficient to represent a high risk. Additional criteria need to be added to require a DPIA. According to the European Data Protection Board in charge of the consistent application of the GDPR across the EU, the processing of biometric data needs to reach the threshold of sensitive data (i.e. the data are processed to uniquely identify an individual) and be accompanied with one of the criteria defined by the A29WP (for instance, the processing operation is carried out on large-scale or involves a systematic monitoring).[27] *Chapter 6* surveyed the provisions of both the GDPR and the 'police' Directive and made recommendations in the context of law enforcement reprocessing of biometric data collected by private parties. In the end, if a DPIA is a good tool to compensate for the absence of the obligation of transparency (as a DPIA describes how the data will be managed), it cannot replace the right to information. It can, nonetheless, recommend the adoption of procedures to inform individuals that law enforcement authorities have accessed their personal data.

**In a nutshell,** the research has established that the EU data protection rules do not provide adequate safeguards to individuals when their biometric data collected under the GDPR are reprocessed under the 'police' Directive rules. In particular, through an analogy based on the ECJ's interpretation of data retention legislation, it appears that the 'police' Directive lacks clarity, in particular, on the scope of the right to information. The role played by the principle of purpose limitation in the scenario of processing operations across the two instruments is also uncertain. Beyond the safeguards, the research has uncovered a significant terminological issue on the concept of biometric data. The issue has an impact on the processing of biometric data not only by law enforcement authorities but also by private or public parties processing biometric data for various purposes.

So, what are the solutions? As suggested along the different chapters of the research, several paths could be followed, even if none of them seems to be the ultimate solution. First, the European Data Protection Board, replacing the Article 29 Data Protection Working Party, could issue recommendations and guidelines to clarify the scope of the rules. This would be very beneficial to clarify the notion of 'biometric data' and the conditions under which biometric data are considered sensitive data, in particular for the biometric industry. There is also guidance needed on the rules applicable to personal data processing across the two instruments. However, as a downside, the Board's guidelines and recommendations are non-binding. Second, since Directive 2016/680 has been implemented in Member States, national courts could send preliminary questions to the ECJ based on national provisions. If this path is the best to ensure legal certainty, it might


[27] EDPB, Opinions on data protection authorities' DPIA draft lists [2018] <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en>accessed 30 December 2018.

be long and might also require the zeal of an activist citizen to start legal proceedings at national level.

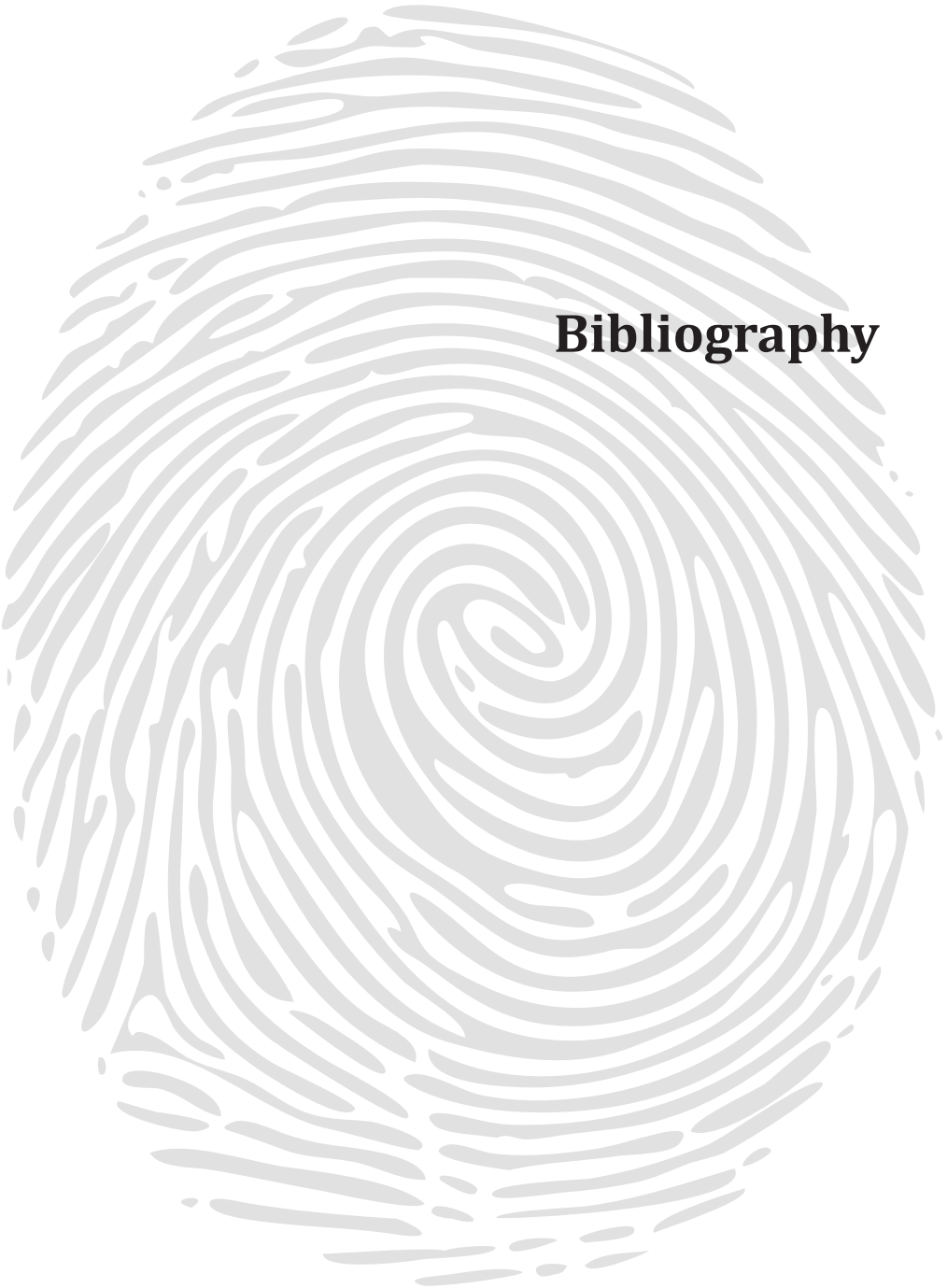
***What's next?***

The study made for this dissertation constitutes groundwork for future research. Several of the provisions that the research has interpreted are new and still untested, in particular the provisions of the 'police' Directive.[28] The scenario at the origin of the research has also evolved during the research: it started with the volume of biometric data collected by private parties for biometric solutions and moved to the trove of 'personal data' (photographs, voice samples) held by social media that could be reprocessed for biometric recognition purposes.[29] In some respects, the study remains exploratory. Nevertheless, the research would benefit from follow-up studies on several aspects. For instance, it would be very interesting to analyse how Member States have implemented the provisions of the 'police' Directive, and in particular the principle of purpose limitation, and whether any Member State has solved the issue of the reprocessing of personal data across instruments (or across fields). Likewise, it would be interesting to survey how Member States have transposed Article 13 of the Directive (the right to information) in their national law.

Through the publication of articles, the research has made a selection of issues. However, there is room to explore the differences between the various types of law enforcement purposes based on the impact that these purposes might have on the rights to individuals. The study has briefly sketched the differences between crime investigation –linked to an offence – and crime surveillance –in the absence of offence and suspect.

Last but not least, the study could be completed with case studies, such as a case study on social media mining by law enforcement authorities. The research did not claim that law enforcement authorities could search directly through social media's data troves. But, the issue of the source of data used by the police needs to be explored. Concerning facial images (or voice samples) held by social media, law enforcement authorities can access them through different means: a request to the social media, feeds, or the users themselves making the information publicly available. Such a case study could cover the technical aspects (facial recognition), analyse the impact of the different ways of access on individuals' rights, compare law enforcement purposes (criminal surveillance and criminal investigation), research privacy-preserving solutions, and elaborate a model of data protection impact assessment applicable to social media mining. This dissertation thus paves the way for future interdisciplinary research.

[28] Such as the principle of purpose limitation, the conditions applicable to the further processing of personal data collected for a different purpose, and the scope of the right to information.
[29] See in particular the examples given in the introduction section to *Chapter 5*, which focuses on the amount of personal data (including biometric data) held by social media.



# Bibliography

## *Bibliography*

### I. LEGISLATION

#### A. EU LEVEL

***Treaties and Charters***

Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C306/01

Treaty on the Functioning of the European Union (TFEU), consolidated version [2016] OJ C202/47

Treaty on European Union (TEU), consolidated version [2016] OJ C202/13

Charter of Fundamental Rights of the European Union [2016] OJ C202/389

Explanations relating to the Charter of Fundamental Rights [2007] OJ C303/17

***Regulations, Directives, and Decisions***

***(i) Council***

Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention [2000] OJ L316/1

Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2004] OJ L385/1

Decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC) [2004] OJ L213/5

Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2006] OJ L386/89

Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L205/63

Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L210/1

Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ L210/12

Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Council Framework Decision 2008/977/JHA) [2008] OJ L350/60

Decision of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (2010/412/EU) [2010] OJ L195/3

***(ii) European Parliament and Council***

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of such data (Directive 95/46/EC) [1995] OJ L281/31

Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54

Regulation (EU) No 603/2013 of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast) [2013] OJ L180/1

Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and of the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1

Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimes [2016] OJ L119/32

Regulation (EU) 2016/794 of 11 May 2016 on the European Union Agency for law enforcement cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L135/53

***EU Legislative Proposals and Resolutions***

***(i) Council***

Political agreement on the 'Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data' LIMITE doc. no 7740/15 [2015]

<http://data.consilium.europa.eu/doc/document/ST-7740-2015-INIT/en/pdf > accessed 30 September 2018

***(ii) European Commission***
Draft 'Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data ('Police and Criminal Justice Data Protection Directive')', version 34 [2011]
<http://www.statewatch.org/news/2011/dec/ep-dp-leas-draft-directive.pdf> accessed 30 September 2018

***(iii) European Parliament***
Resolution of 11 February 2015 on anti-terrorism measures' (2015/2530 (RSP)) [2015]
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0032+0+DOC+XML+V0//EN> accessed 1 August 2017

***(iv) European Union and the United States of America***
Agreement on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program [2010] OJ L8/11

### B. COUNCIL OF EUROPE

Convention for the Protection of Human Rights and Fundamental Freedoms [1950]
<https://www.echr.coe.int/Documents/Convention_ENG.pdf> accessed 30 September 2018

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] (ETS No. 108)
<http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm> accessed 30 September 2018

### C. NATIONAL LEVEL

***(i) Australia***
Australian Government, Federal Register of Legislation, Privacy Act 1998
<https://www.legislation.gov.au/Details/C2014C00076> accessed 30 November 2018

***(ii) Belgium***
Belgium Parliament, Law of 30 July 2018 on the Protection of Individuals with regard to the Processing of Personal Data
(*Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*)
<http://www.ejustice.just.fgov.be/cgi/article.pl?language=nl&caller=summary&pub_date=2018-09-05&numac=2018040581> accessed 30 November 2018

***(iii) France***
French Parliament, Law No. 2018-493 of 20 June 2018 on the Protection of Personal Data
(*Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles*)
<https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte> accessed 30 November 2018

***(iv) Netherlands***

Dutch Parliament, Law of 17 October 2018 amending the Police Data Act and the Judicial and Criminal Procedural Act implementing EU rules on the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties
(*Wet van 17 oktober 2018 tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen*)
<https://zoek.officielebekendmakingen.nl/stb-2018-401.html> accessed 30 November 2018

***(v) United Kingdom***

UK Parliament, Data Protection Act 2018
<http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> accessed 30 November 2018

**II. CASE LAW**

**A. EUROPEAN COURT OF JUSTICE**

Case C-292/89 *R v Immigration Appeal Tribunal ex parte Gustaff Desiderius Antonissen* [1991] ECR-I-745

Case C-275/06, *Productores de Música de España (Promusicae)* v *Telefónica de España SAU* [2008] ECLI:EU:C:2008:54

Case C-524/06 *Heinz Huber v Bundesrepublik Deutschland* [2008] ECLI:EU:C:2008:194, Opinion of AG Maduro

Case C-301/06, *Ireland v European Parliament and Council* [2009] ECLI:EU:C:2009:68

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Hartmut Eifert v Land Hessen* [2010] ECLI:EU:C:2010:662

Case C-291/12 *Michael Schwarz v Stadt Bochum* [2013] EU:C:2013:401, Opinion of AG Mengozzi

Case C-291/12 *Michael Schwarz v Stadt Bochum* [2013] ECLI:EU:C:2013:670

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECLI:EU:C:2014:238

Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650

Joined Cases C-446/12 to V-449/12 *WP Willems and others* [2015] ECLI:EU:C:2015:238

Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and others* [2016] ECLI:EU:C: 2016:572, Opinion of AG Saudmandsgaard ØE

Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and others* [2016] ECLI: EU:C:2016:970

*Opinion 1/15 of the Court (Grand Chamber) on the Draft Agreement between Canada and the European Union* [2017], ECLI:EU:C:2016:656

### B. EUROPEAN COURT OF HUMAN RIGHTS

*Handyside v UK App* no 5493/73 (ECHR, 7 December 1976)

*Klass and others v Germany* App no 5029/71 (ECHR, 6 September 1978)

*Malone v the United Kingdom* App no 8691/79 (ECHR, 2 August 1984)

*Leander v Sweden* App no 9248/81 (ECHR, 26 March 1987)

*Amann v Switzerland* App no 27798/95 (ECHR, 16 February 2000)

*Rotaru v Romania* App no 28341/95 (ECHR, 4 May 2000)

*Khan v UK* App no 35394/97 (ECHR, 12 May 2000)

*Connors v the United Kingdom* App no 66746/01 (ECHR, 27 May 2004)

*Weber and Saravia v Germany* App no 54934/00 (ECHR, 29 June 2006)

*Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* App no 62540/00 (ECHR, 28 June 2007)

*S and Marper v the United Kingdom* App nos 30562/04 and 30566/04 (ECHR, 4 December 2008)

*M K v France* App no 19522/09 (ECHR, 18 April 2013)

*Roman Zakharov v Russia* App no 47143/06 (ECHR, 4 December 2015)

*Szabó and Vissy v Hungary* App no 37138/14 (ECHR, 12 January 2016)

## III. GUIDELINES, OPINIONS, AND RECOMMENDATIONS

### A. EU LEVEL

***(i) Article 29 Data Protection Working Party***

Working Document on biometrics [2003] WP80

Opinion No. 7/2004 on the inclusion of biometric elements in the residence permits and visa taking account of the establishment of the European information system on visas (VIS) [2004] WP96

Opinion 3/2005 on implementing the Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travelled documents issued by Member States [2005] WP112

Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] WP119

Opinion 4/2007 on the concept of personal data [2007] WP136

'The Future of Privacy', Joint contribution with the Working Party on Police and Justice to the Consultation of the European Commission on the legal framework to the fundamental right to protection of personal data, WP 168 [2009]

Opinion 3/2010 on the principle of accountability [2010] WP173

Advice Paper on Special Categories of Data ('Sensitive Data') [2011] Ref. Ares (2011) 444105

Opinion 02/2012 on facial recognition in online and mobile services [2012] WP192

Opinion 3/2012 on development in biometric technologies [2012] WP193

Opinion 03/2013 on purpose limitation [2013] WP203

Opinion 05/2013 on Smart Borders [2013] WP206

Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (2014) WP211

Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes' [2014] WP215

Statement on the role of a risk-based approach in data protection legal frameworks [2014] WP218

Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention,

investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data [2015] WP233

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ' likely to result in a high risk ' for the purposes of Regulation 2016/679 [2018] WP248 rev.01

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 [2018] WP251 rev.01

***(ii) Council***

Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Preparation for a general approach 9565/15 (11 June 2015) [2015]
<https://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf> accessed 20 July 2015

***(iii) European Commission***

Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM (2007) 228 final [2007]
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0228&from=EN> accessed 30 September 2018

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee of the Regions: A Comprehensive Approach to Personal Data Protection in the European Union' COM (2010) 609 final
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2010:0609:FIN> accessed 30 September 2018

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, 2012/0011 (COD) [2012]
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN> accessed 30 September 2018

Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final, 2012/0010 (COD) [2012]
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=en> accessed 30 September 2018

Impact Assessment accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for

the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC (2012) 72 final [2012]
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=en> accessed 20 July 2015

'Answer to the Resolution of the European Parliament of 11 February 2015 concerning the consequences of the judgment of the Court of Justice on the Data Retention Directive and its possible impact on the proposed EU Directive on Passenger Name Records (PNR)' (leaked document) [2015]
<http://statewatch.org/news/2015/mar/eu-com-eu-pnr-letter.pdf> accessed 30 September 2018

***(iv) European Data Protection Board***

Endorsement 1/2108 [2018]
<https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents.pdf> accessed 30 September 2018

'Europe's new data protection rules and the EDPB: giving individuals greater control' (press release, 25 May 2018)
< https://edpb.europa.eu/news/news/2018/europes-new-data-protection-rules-and-edpb-giving-individuals-greater-control_en > accessed 30 December 2018

Opinion 5/2018 on the draft list of the competent supervisory authority of Germany regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR) [2018]
<https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52018-germany-sas-dpia-list_en> accessed 30 December 2018

Opinion 13/2018 on the draft list of the competent supervisory authority of Lithuania regarding the processing operations subject to the requirements of a data protection impact assessment (Article 35.4 GDPR) [2018]
<https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_lt_sas_dpia_list_en.pdf > accessed 30 December 2018

Opinion 16/2018 on the draft list of the competent supervisory authority of the Netherlands regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR) [2018]
<https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_nl_sas_dpia_list_en.pdf> accessed 30 December 2018

Opinion 22/2018 on the draft list of the competent supervisory authority of the United Kingdom regarding the processing operations subject the requirement of a data protection impact assessment (Article 35.4 GDPR) [2018]
<https://edpb.europa.eu/sites/edpb/files/files/file1/2018-09-25-opinion_2018_art._64_uk_dpia_list_en.pdf > accessed 30 December 2018

***(v) European Data Protection Supervisor***

Opinion on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final) [2005] OJ C181/13

Opinion on the Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II) (COM(2005) 230 final); the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system

(SIS II) (COM(2005) 236 final), and the Proposal for a Regulation of the European Parliament and of the Council regarding access to the second generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM (2005) 237 final) [2005] OJ C91/38

Opinion on the Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM (2005) 600 final) [2006] OJ C97/6

Opinion on the draft Council Regulation (EC) laying down the form of the laissez-passer to be issued to members and servants of the institutions [2006] OJ C313/36

Opinion of the European Data Protection Supervisor on the modified proposal for a Council Regulation amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals [2006] OJ C320/21

Comments on the Communication of the Commission on interoperability of European databases [2006]
<https://edps.europa.eu/sites/edp/files/publication/06-03-10_interoperability_en.pdf> accessed 30 May 2016

Opinion on the Initiative of the Federal Republic of Germany, with a view to adopting a Council Decision on the implementation of Decision 2007/…/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [2008] OJ C89/1

Opinion on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States [2008] OJ C 200/1

Opinion on the Communication from the Commission to the European Parliament and the Council on an area of freedom, security and justice serving the citizen [2009] OJ C276/09

Video Surveillance Guidelines [2010]
<https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf> accessed 30 September 2018

Opinion on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (.../...) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes [2010] OJ C92/1

Opinion on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs) [2011]
<https://edps.europa.eu/sites/edp/files/publication/11-02-01_fp7_en.pdf> accessed 20 July 2015

Opinion on the data protection reform package [2012]
<https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf> accessed 30 September 2018

Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration [2012] OJ C34/18

Opinion on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] [...] (Recast version) [2012]
<https://edps.europa.eu/sites/edp/files/publication/12-09-05_eurodac_en.pdf> accessed 30 September 2018

Opinion 5/2015, Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2015]
<https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf> accessed 10 April 2018

Developing a "Toolkit" for Assessing the Necessity of the Measures that Interfere with Fundamental Rights (Background Paper for consultation) [2016]
<https://edps.europa.eu/sites/edp/files/publication/16-06-16_necessity_paper_for_consultation_en.pdf> accessed 10 April 2018

'EDPS launches Accountability Initiative' [2016], factsheet
<https://edps.europa.eu/sites/edp/files/publication/16-06-07_accountability_factsheet_en.pdf> accessed 30 September 2018

Opinion 06/2016, EDPS Opinion on the Second EU Smart Borders Package, Recommendations on the revised Proposal to establish an Entry/Exit System [2016]
<https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_en.pdf> accessed 30 September 2018

Opinion 07/2016, EDPS Opinion on the First reform package on the Common European Asylum System (Eurodac, EASO and Dublin regulations) [2016]
<https://edps.europa.eu/sites/edp/files/publication/16-09-21_ceas_opinion_en.pdf> accessed 30 September 2018

Assessing the necessity of measures that limit the fundamental right to data protection: A toolkit [2017]
<https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf> accessed 10 April 2018

Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems [2018]
<https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf> accessed 30 September 2018

Opinion 05/2018, Preliminary Opinion on Privacy by Design [2018]
<https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf> accessed 30 September 2018

***(vi) European Network and Information Society Agency***
Privacy and Data Protection by Design- from Privacy to Engineering (Report 2014)
<https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> accessed on 30 September 2018

***(vii) European Parliament***
Draft report on 'the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' (Albrecht JP (rapporteur)) [2013] PE 506.145v01-00
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-506.145+01+DOC+PDF+V0//EN&language=EN> accessed 20 July 2015

Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM (2012) 0011- C7-0025/2012 – 2012/0011 (COD) PT7_TA(2014) 01 [2014]
<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402> accessed 20 July 2015

Legislative Resolution on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM (2012) 0010 – C7-0024/2012 -2012/0010 (COD)), P7_TA(2014)0219 [2014]
<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0219> accessed 20 July 2015

Legal Opinion of the Legal Service, leaked document, 'LIBE- Questions relating to the judgment of the Court of Justice of 8 April 2014 in joined cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others*- Directive 2006/24/EC on data retention- Consequences of the judgment'
<http://www.statewatch.org/news/2015/apr/ep-ls-opinion-digital-rights-judgment.pdf> accessed 30 September 2018

***(viii) European Union Agency for Fundamental Rights***
Handbook on European Data Protection Law [2014]
<http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law-2014-edition> accessed 30 September 2018

Handbook on European Data Protection Law [2018]
<http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law> accessed 30 September 2018

**B. COUNCIL OF EUROPE LEVEL**

***(i) Council of Europe***
Recommendation No. R(87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector [1987]
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e7a3c> accessed 30 September 2018

***(ii) Consultative Committee of Convention 108***
Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data [2005]
<https://rm.coe.int/16806840ba> accessed 30 September 2015

Draft Practical Guide on the Use of Personal Data in the Police Sector, T-PD(2016)02rev5 [2017]

Practical Guide on the Use of Personal Data in the Police Sector T-PD(2018)01 [2018]

Draft Explanatory Report of the Modernised Version of Convention 108' (based on the proposals adopted by the 29th Plenary meeting of the T-PD), TP-PD- BUR (2013) 3ENrev5 [2013]

***(iii) Directorate of the Jurisconsult***
'Guide on Article 8 of the European Convention on Human Rights, Right to Respect for Private and Family Life, Home and Correspondence' [2018]
<https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed 30 September 2018

***(iv) Parliamentary Assembly of the Council of Europe***
Committee on Legal Affairs and Human Rights, 'The Need for a Global Consideration of the Human Rights Implications of Biometrics' (2011) Rapporteur H Haibach, Doc 12 522
<https://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=13103&lang=en>accessed 20 July 2015

Recommendation 1960 (2011), 'The Need for a Global Consideration of the Human Rights Implications of Biometrics'
<https://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=17964&lang=en>accessed 20 July 2015

Resolution 1797 (2011), 'The Need for a Global Consideration of the Human Rights Implications of Biometrics'
<https://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=17968&lang=en>accessed 20 July 2015

**C. INTERNATIONAL LEVEL**

***(i) International Civil Aviation Organization***
Guidelines on Passenger Name Record (PNR) Data, first edition 2010, Doc 9944
<https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf > accessed on 30 September 2018

***(ii) International Conference of Data Protection and Privacy Commissioners***
Resolution on the Use of Biometrics in Passports, Identity Cards and Travel Documents, 27th Conference, Montreux, 16 September 2005 [2005]
<https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Use-of-Biometrics-in-passports-identity-cards-and-travel-documents.pdf> accessed 20 July 2015

Resolution on Privacy by Design, Jerusalem, Israel, 32nd Conference [2010]

<https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf> accessed 30 September 2018

***(iii) Organisation for Economic Cooperation and Development***
Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [1980] (updated in 2013)
<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 30 September 2018

**D. NATIONAL LEVEL**

***(i) Belgium***
***Autorité de Protection des Données***
Recommendation n°01/2018 du 28 février 2018, [2018] 43
<https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_01_2018.pdf> accessed on 30 September 2018

***(ii) France***
***Commission Nationale Informatique et Libertés***
Privacy Impact Assessment (PIA): Knowledge Bases [2018]
<https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-enknowledgebases.pdf>
accessed 30 September 2018

Privacy Impact Assessment (PIA): Templates [2018]
<https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf>
accessed 30 September 2018

'CNIL publishes an update of its PIA Guides' (*cnil.fr*, 26 February 2018)
<https://www.cnil.fr/en/cnil-publishes-update-its-pia-guides> accessed 30 September 2018

***(iii) Italy***
***Il Garante***
Guidelines on Biometric Recognition and Graphometric Signature, Annex A to the Garante's Order of 12 November 2014 [2014]
<http://194.242.234.211/documents/10160/0/GUIDELINES+ON+BIOMETRIC+RECOGNITION>
accessed 20 July 2015

***(iv) United Kingdom***
***Dyfed Powys Police***
Data Protection Impact Assessment Policy
<https://www.dyfed-powys.police.uk/media/5874/data-protection-impact-assessment-policy.pdf> accessed 30 December 2018

***Information Commissioner's Office***
Guide to the General Data Protection Regulation (GDPR) [2018]
<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf> accessed on 30 September 2018

Guide on 'Accountability and Governance: Data Protection Impact Assessments (DPIAs)' [2018]

<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf> accessed 30 September 2018

Sample DPIA Template [2018]
<https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf> accessed 30 September 2018

***Parliament***
Data Protection Bill, Bill 190 2017-19, as amended in Public Bill Committee (23 March 2018)
<https://publications.parliament.uk/pa/bills/cbill/2017-2019/0190/18190.pdf > accessed 10 April 2018

***(v) Ireland***
***Data Protection Commissioner***
Guidance on Biometrics in the Workplace
<https://www.dataprotection.ie/docs/Biometrics-in-the-workplace/m/244.htm> accessed 30 September 2018

***(vi) Netherlands***
***Tweede Kamer (Second chamber, Parliament)***
Dutch draft law to implement Directive 2016/680 (16 February 2018) (*Voorstel van Wet* n°34889-2- *Wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen*)
<https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?cfg=wetsvoorsteldetails&qry=wetsvoorstel:34889> accessed 10 April 2018

**IV. STANDARDS AND GLOSSARIES**

***(i) Association for Biometrics and International Computer Security Association***
'1999 Glossary of Biometric Terms'
<biometrics3.tripod.com/pubs/glossary.pdf> accessed 20 July 2015

***(ii) International Organization for Standardization***
ISO/IEC 2382-37: 2012 (E)- Information Technology- Vocabulary- Part 37: Biometrics,
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55194> accessed 20 July 2015

***(iii) US National Science and Technology Council's Subcommittee on Biometrics***
Biometrics Glossary [2006]
<http://www.biometrics.gov/documents/glossary.pdf> accessed 20 July 2015

## V. LITERATURE

### *(i) Books and Book Chapters*

Adler A and Schuckers S, 'Biometric Vulnerabilities, Overview' in Li S and Jain A (eds), *Encyclopedia of Biometrics* (Springer 2015)

Alexander L and Sherwin E, *Demystifying Legal Reasoning* (Cambridge University Press 2008)

Barnard C and Peers S, *European Union Law* (1st edn, OUP 2014)

Brems E and Gerards J (eds), *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (Cambridge University Press 2014)

Boehm F, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level* (Springer 2012)

Campisi P (ed), *Security and Privacy in Biometrics* (Springer 2013)

Cannataci J, Caruana M, and Mifsud Bonnici J, 'R (87) 15: A Slow Death?' in Kleve P, De Mulder R and van Noortwijk C (eds), *Monitoring, Supervision and Information Technology, Proceedings of the First International Seminar of the Legal Framework Society (LEFIS)* (Erasmus University Press 2007)

Cate F and Dempsey J (eds), *Bulk Collection, Systematic Government's Access to Private Sector Data* (OUP 2017)

Cavoukian A, 'Privacy by Design: Take the Challenge' (Information and Privacy Commissioner of Ontario, 2009)

Chen Y and Fondeur JC, 'Biometric Algorithms' in Li S and Jain A (eds), *Encyclopedia of Biometrics* (Springer, 2015)

Cole S, *Suspect Identities: A History of Fingerprinting and Criminal Identification* (Harvard University Press 2001)

Colonna L, 'Data Mining and its Paradoxical Relationship to the Purpose of Limitation' in Gutwirth G, Leenes R and De Hert P (eds), *Reloading Data Protection* (Kluwer 2014)

De Busser E, *Data Protection in EU and US criminal cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities* (Maklu 2009)

De Busser E and Vermeulen G, 'Towards a Coherent EU Policy on Outgoing Data Transfers for Use in Criminal Matters? The Adequacy Requirement and the Framework Decision on Data Protection in Criminal Matters. A Transatlantic Exercise in Adequacy' in Cools M et al (eds), *EU and International Crime Control*, *Topical Issues*, Governance and Security Research Paper Series vol. 4 (Maklu 2010)

De Hert P, 'Division of Competencies between National and European Levels with Regard to Justice and Home Affairs' in Apap J (ed), *Justice and Home Affairs in the EU: Liberty and Security Issues after Enlargement* (Elgar, 2004)

De Hert P and Boehm F, 'The Rights of Notification After Surveillance is Over: Ready for Recognition?' (2012) Digital Enlightenment Yearbook 19

De Hert P and Gutwirth S, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Claes E, Duff A, and Gutwirth S (eds), Privacy and the Criminal Law (Intersentia 2006)

De Hert and Malgieri G, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but not Necessarily by Judges' in Gray D and Henderson S (eds), *Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017)

Dempsey J, Cate H, and Abrams M, 'Organizational Accountability, Government Use of Private-Sector Data, National Security, and Individual Privacy' in Cate F and Dempsey J (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data* (OUP 2017)

González Fuster G, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014)

Gutwirth S, Poullet Y, De Hert P, de Terwangne C, and Nouwt S (eds), *Reinventing Data Protection?* (Springer 2009)

Gutwirth S, Leenes L, and De Hert P (eds), *Reloading Data Protection* (Springer 2014)

Hansen M, 'Data Protection by Default in Identity-Related Applications' in Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell (eds), *Policies and Research in Identity Management* (Springer 2013)

Hijmans H, *The European Union as Guardian of Internet Privacy and Data Protection: The Story of Art 16 TFEU* (Springer 2016)

Hustinx P, 'European Leadership in Privacy and Data Protection' in Rallo Lombarte A and García Mahamut R (eds), *Hacia un Nuevo Derecho European de Protección de Datos, Towards a New European Data Protection Regime* (Tirant lo Blanch 2015)

Jain A, Ross A, and Nandakumar K (eds), *Introduction to Biometrics* (Springer 2011)

Jain A, Flynn P, and Ross A (eds), *Handbook of Biometrics* (Springer 2008)

Kindt E, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis* (Springer 2013)

Klip A (ed), *Substantive Criminal Law of the European Union* (Maklu 2011)

Klip A, *European Criminal Law: An Integrative Approach* (3rd edn, Intersentia 2016)

Klitou D, *Privacy-Invading and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century* (Springer 2014)

Kotschy W, 'Article 2, Directive 95/46/EC' in Büllesbach A, Gijrath S, Poullet Y, and Prins C (eds), *Concise of European IT law* (2nd edn, Kluwer Law International 2010)

Kranenborg H, 'Article 8' in Peers S et al (eds), *The EU Charter of Fundamental Rights, A Commentary* (Hart Publishing 2014)

Kumar A and Zhang D (eds), *Ethics and Policy of Biometrics,* Third International Conference on Ethics and Policy of Biometrics and International Data Sharing, IECB (Springer 2010)

Kuner C, Bygrave L, and Docksey C (eds), 'Draft commentaries on 10 GDPR articles,' in *Commentary on the EU General Data Protection Regulation* (OUP 2019)

Kung A, 'PEARS: Privacy Enhancing Architectures' in Preneel B and Ikonomou D (eds), *Privacy Technologies and Policies* (Springer 2014)

Lessig L, 'Code, Version 2.0' (Basic Books 2006)

Li S and Jain A (eds), *Handbook of Face Recognition* (2nd edn, Springer 2011)

Li S and Jain A (eds), *Encyclopedia of Biometrics* (Springer 2015)

Liu NY, *Bio-Privacy, Privacy Regulations and the Challenges of Biometrics* (Routledge 2012)

Lowrance W, 'Privacy, Confidentiality, Safeguards' in *Privacy, Confidentiality, and Health Research* (Cambridge University Press 2012)

Lynskey O, *The Foundations of EU Data Protection Law* (OUP 2015)

Lynskey O, 'The Role of Collective Actors in the Enforcement of the Right to Data Protection under EU Law' in Muir E, Kilpatrick C, Miller J, and de Witte B (eds), *How EU Shapes Opportunities for Preliminary References on Fundamental Rights: Discrimination, Data Protection and Asylum* (2017) EUI Working Paper Law 2017/17

Maltoni D, 'Fingerprint Recognition, Overview' in Li S and Jain K (eds), *Encyclopedia of Biometrics* (Springer 2015)

Maltoni D, Maio D, Jain A, and Prabhakar S (eds), *Handbook of Fingerprint Recognition* (2nd edn, Springer 2009)

Mann T (ed), *Australian Law Dictionary* (OUP 2010)

McBride J, *Human Rights and Criminal Procedure: The Case Law of the European Court of Human Rights* (2nd edn, Council of Europe 2018)

McIver R, 'Biometric Vocabulary Standardization' in Li S and Jain A (eds), *Encyclopedia of Biometrics* (Springer 2015)

Mifsud Bonnici J, 'Redefining the Relationship Between Security, Data Retention and Human Rights' in Holzhacker R and Luif P (eds), *Freedom, Security and Justice in the European Union* (Springer 2014)

Mitsilegas V, *EU Criminal Law after Lisbon: Rights, Trust and the Transformation of Justice in Europe* (Hart Studies 2018)

Pato JN and Millett LI (eds), *Biometric Recognition: Challenges and Opportunities,* Whither Biometrics Committee and National Research Council (The National Academies Press 2010)
Peers S, EU Justice and Home Affairs Law: Volume II: EU Criminal Law, Policing, and Civil Law (Oxford 2016)

Peers S, Hervey T, Kenner J, and Ward A (eds)*, The EU Charter of Fundamental Rights, A Commentary* (Hart Publishing 2014)

Peers S and Prechal S, 'Article 52' in S Peers et al (eds), *The EU Charter of Fundamental Rights, A Commentary* (Hart Publishing 2014)

Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Gutwirth S et al (eds), *Reinventing Data Protection?* (Springer 2009)

Rubinstein I, Nojeim G, and Lee L, 'Systematic Government Access to Private-Sector Data, A Comparative Analysis' in Cate C and Dempsey J (eds), *Bulk Collection, Systematic Government's Access to Private Sector Data* (OUP 2017)

van der Schyff G, 'Interpreting the Protection Guaranteed by Two-Stage Rights in the European Convention on Human Rights, the Case for Wide Interpretation' in Brems E and Gerards J (eds), *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (Cambridge University Press 2014)

Terstegge J, 'Article 3, Directive 95/46/EC,' in Büllesbach A, Gijrath S, Poullet Y, and Prins C (eds), *Concise of European IT law* (2nd edn, Kluwer Law International 2010)

Tzanou M, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing 2017)

Vervaele J, 'Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System' in Gutwirth S, Leenes L, and De Hert P (eds), *Reloading Data Protection* (Springer 2014)

Wayman J, 'Biometric Verification/Identification/Authentication/Recognition:
The Terminology' in S Li and A Jain (eds), *Encyclopedia of Biometrics* (Springer 2015)

***(ii) Articles***

Andoulsi I, 'Personal Data Protection and the First Implementation Semester of the Lisbon Treaty: Achievements and Prospects' (2010) 1 New Journal of European Criminal Law 362

Arestis G, 'Fundamental Rights in the EU: Three Years after Lisbon, the Luxembourg Perspective' (2013)
<http://aei.pitt.edu/43293/1/researchpaper_2_2013_arestis_lawpol_final.pdf> accessed 30 September 2018

Boehm F, 'Data Processing and Law Enforcement Access to Information Systems at EU Level' (2012) 36(5) Datenschutz und Datensicherheit 339

Brkan M, 'In Search of the Concept of Essence of EU Fundamental Rights through the Prism of Data Privacy' (2017) 2017-01 Maastricht Faculty of Law Working Paper 1
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2900281> accessed 30 September 2018

Bordallo Lopez M et al, 'Kinship Verification from Facial Images and Videos: Human versus Machine' (2018) 29(5) Machine Vision and Applications 873

Buitelaar, J C, 'Privacy: Back to the Roots' (2012) 13(3) German Law Journal 171

Bygrave L, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 4(2) Oslo Law Review 105

Cao K and Jain A, 'Learning Fingerprint Reconstruction: from Minutiae to Image' (2015) 10(1) IEEE Transactions on Information Forensics and Security 104

Cannataci J, 'Lex Personalitis & Technology-driven Law' (2008) 5(1) SCRIPT-ed 1
<https://script-ed.org/wp-content/uploads/2016/07/5-1-Cannataci.pdf> accessed 30 September 2018

Cannataci J and Mifsud Bonnici J, 'The End of Purpose-Specification Principle in Data Protection?' (2010) 24 (1) International Review of Law 110

Caruana M, 'The Reform of the EU Data Protection Framework in the Context of Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement' (2017) International Law Review, Computers and Technology
<https://www.tandfonline.com/doi/abs/10.1080/13600869.2017.1370224> accessed 30 September 2018

Chiang CL and Zelen M, 'What is Biostatistics?' (1985) 14 (3) Biometrics 771

Cocq C, '*Information* and *Intelligence*: The Current Divergences between National Legal Systems and the Need for Common (European) Notions' (2017) 8(3) New Journal of European Criminal Law 352

Cocq C and Galli F, 'The Catalysing Effect of Serious Crime on the Use of Surveillance Technologies for Prevention and Investigation Purposes' (2013) 4(3) New Journal of European Criminal Law 256

Costa L and Poullet Y, 'Privacy and the Regulation of 2012' (2012) 28(3) Computer Law and Security Review 254

Coudert F, 'The Europol Regulation and Purpose Limitation: From the 'Silo-Based Approach' to…What Exactly?' (2017) 3(3) EDPL 313

Custers B and Ursic H, 'Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection' (2016) 6(1) International Data Privacy Law 4

De Hert P, 'Balancing Security and Liberty within the European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11' (2005) 1(1) Utrecht Law Review 68

De Hert P and Papakonstantinou V, 'The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters – A Modest Achievement However Not the Improvement Some Have Hoped For' (2009) 25(5) Computer Law and Security Review 403

De Hert P and Papakonstantinou V, 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) 7(1) New Journal of European Criminal Law 7

De Hert P and Riehle C, 'Data Protection in the Area of Freedom, Security and Justice. A Short Introduction and Many Questions Left Unanswered' (2010) 11 (2) ERA Forum 159

Fournier NA and Ross AH, 'Sex, Ancestral, and Pattern Type Variation of Fingerprint Minutiae: A Forensic Perspective on Anthropological Dermatoglyphics' (2016) 160(4) American Journal of Physical Anthropology 625

Friedman B, 'Value Sensitive Design' (1996) Interactions, November-December 17

Galli F, 'Digital Rights Ireland as an Opportunity to Foster a Desirable Approximation of Data Retention Provisions' (2016) 23(3) Maastricht Journal 460

Gellert R, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34(2) Computer Law and Security Review 279

Granger MP and Irion K, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 39(6) European Law Review 835

Grijpink J, 'Privacy Law: Biometrics and Privacy' (2001) 17(3) Computer Law and Security Review 154

Hijmans H and Scirocco A, 'Shortcomings in EU Data Protection in the third and second pillars. Can the Lisbon Treaty be expected to help?' 46(5) Common Market Law Review 1485

Hildebrandt M and Tielemans L, 'Data Protection by Design and Technology Neutral Law' (2013) 29 (5) Computer Law and Security Review 509

Hornung G and Schnabel C, 'Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination' (2009) 25(1) Computer Law and Review 84

Hutchinson T and Duncan N, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17(1) Deakin Law Review 83

Iglesias Sanchez S, 'The Court and the Charter: The Impact of the Entry into Force of the Lisbon Treaty on the ECJ's Approach to Fundamental Rights' (2010) 49 Common Market Law Review 1565

Jain A, 'Biometric Authentication' (2008) 3 (6) Scholarpedia 3716

Jain A, Ross A, and Prabhakar 'An Introduction to Biometric Recognition' (2004) 14(1) IEEE Transactions on Circuits and Systems for Video Technology 4

Jasmontaite L, Kamara I, Zanfir Fortuna, G, and Leucci, S, 'Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR' (2018) 4(2) EDPL 168

Kahn H et al, 'A Fingerprint Marker from Early Gestation Associated with Diabetes in Middle Age: the Dutch Hunger Winter Families Study' (2009) 38(1) International Journal of Epidemiology 101

Kaye D, 'Questioning a Courtroom Proof of the Uniqueness of Fingerprints' (2003) 71(3) International Statistical Review 521

Kindt E, 'Biometric Application and the Data Protection Legislation: The Legal Review and Proportionality Test' (2007) 31(3) Datenschutz und Datensicherheit 166

Kindt E, 'Having Yes, Using No? About the New Legal Regime for Biometric Data' (2018) 34(3) Computer Law and Security Review 433

Kokott J and Sobotta C, 'The Distinction between Privacy and Data Protection Jurisprudence of the CJEU and the ECtHR' (2013) International Data Privacy Law 22

Kokott J and Sobotta C, 'The Charter of Fundamental Rights of the European Union after Lisbon,' EUI Working Papers' (2016) 6 AEL

Kuner C, Cate FH, Millard C, and Svantesson DJ, 'The Challenge of "Big Data" for Data Protection' (2012) 2(2) International Data Privacy Law 47

Lazaro C and Le Métayer D, 'The Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12(1) SCRIPT-ed 3
<https://script-ed.org/wp-content/uploads/2015/06/lazaro_metayer.pdf> accessed 30 September 2018

van Lieshout M, Kool L, van Schoonhoven B, and de Jonge M, 'Privacy by Design: An Alternative to Existing Practice In Safeguarding Privacy' (2011) 13(6) Info 55

Liu NY, 'Identifying Legal Concerns in the Biometric Context' (2008), 3(1) Journal of International Commercial Law and Technology 45

Lynskey O, 'The *Europeanisation* of Data Protection Law' (2017) 19 Cambridge Yearbook of European Legal Studies 252

Marquenie T, 'The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework (2017) 33 (3) Computer Law and Security Review 324

Mayer J, Mutchler P, and Mitchell JC, 'Evaluating the Privacy Properties of Telephone Metadata' (2013) 113 (20) Proceedings of the National Academy of Sciences of the United States of America 5536

Mifsud Bonnici J, 'Exploring the Non-Absolute Nature of the Right to Data Protection' (2014) 28(2) International Review of Law, Computers and Technology 131

van Ooik R, 'Cross-Pillar Litigation Before the ECJ: Demarcation of Community and Union Competences' (2008) 4 (3) European Constitutional Law Review 399

Prabhakar S, Pankanti S, and Jain A, 'Biometric Recognition: Security and Privacy Concerns' (2003) 1 (2) IEEE Security and Privacy 33

Prins C, 'Biometric Technology Law, Making Our Body Identify for us: Legal Implications of Biometric Technologies' (1998) 14(3) Computer Law and Security Report 159

Purtova N, 'Between the GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships' (2018) 8(1) International Data Privacy Law 52

Reding V, 'The European Data Protection Framework for the Twenty-First Century' (2012) 2(3) International Data Privacy Law 119

Ritleng D, 'The Contribution of the Court of Justice to the Structuring of the European Space of Fundamental Rights' (2014) 5(4) New Journal of European Criminal Law 507

Ross A, Shah J, and Jain A, 'From Template to Image: Reconstructing Fingerprints from Minutiae Points' (2007) 29(4) IEEE Transactions on Patterns Analysis and Machine Intelligence 544

Rubinstein I, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3(2) International Data Privacy Law 74

Rubinstein I and Good N, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2013) 28 Berkeley Technology Law Journal 1133

Saks M, 'Forensic Identification: From a Faith-Based 'Science' to a Scientific Science' (2010) 201(1-3) Forensic Science International 14

Samuel G, 'Can Legal Reasoning be Demystified?' (2009) 29(2) Legal Studies 181

Schaar P, 'Privacy by Design' (2010) 2(3) Identity in the Information Society 267

Scirocco A, 'The Lisbon Treaty and the Protection of Personal Data in the European Union' (2008) 5 Data Protection Review

Schrama W, 'How to Carry out Interdisciplinary Legal Research: Some Experiences with an Interdisciplinary Research Method' (2011) 7(1) Utrecht Law Review 147

Shapiro S, 'Privacy by Design: Moving from Art to Practice' (2010) 53(6) Communications of the ACM 27

Spiekermann S and Cranor L, 'Engineering Privacy' (2009) 35(1) IEEE Transactions on Software Engineering 67

Stiegler S, 'The Problematic Unity of Biometrics' (2000) 56 Biometrics 653

Taekema H, 'Theoretical and Normative Frameworks for Legal Research: Putting Theory into Practice' (2018) 1 Law and Method
<https://www.bjutijdschriften.nl/tijdschrift/lawandmethod/2018/02/lawandmethod-D-17-00010> accessed 30 September 2018

Taylor J and Blenkin M, 'Uniqueness in the Forensic Identification Sciences: Fact or Fiction?' (2011) 206 (1-3) Forensic Science International 12

Tzanou M, 'Data Protection as a Fundamental Right next to Privacy? *Reconstructing* a not so New Right' (2013) 3(2) International Data Privacy Law 88

Walker E, 'Biometrics Boom: How the Private Sector Commodifies Human Characteristics' (2015) 25 (3) Fordham Intellectual Property Media and Law 831

Zorkadis V and Donos P, 'On Biometrics-Based Authentication and Identification from a Privacy-Protection Perspective: Deriving Privacy-Enhancing Requirements' (2004) 12 IMCS 125

***(iii) Working Papers and Conference Papers***

Butin D and Le Métayer D, 'Log Analysis for Data Protection Accountability' in Jones C, Pihlajasaari, and Sun J (eds) FM 2014, Formal Methods, International Symposium on Formal Methods (Springer 2014) 163

De Hert P and Christianen K, 'Report on the Application of the Principles of Convention108 to the Collection and Processing of Biometric Data' *Commissioned by the Council of Europe* (2013)

Hoepman JH, 'Privacy Design Strategies', Proceedings ICT Systems Security and Privacy Protection- 29th IFIP TC 11 International Information Security Conference (SEC 2014)
<https://hal.inria.fr/hal-01370395/document> accessed 30 September 2018

Jasserand C, 'Legal Perspectives on the Difficult Relationship between the Concept of Privacy by Design and the Principle of Purpose Limitation at European Level' (Amsterdam Privacy Conference 2015)

Kemelmacher-Shlizerman I, Seitz S, Miller D and Brossard E, 'The MegaFace Benchmark: 1 Million Faces for Recognition at Scale' (2015)
<https://arxiv.org/abs/1512.00596> accessed 30 September 2018

Kloza D et al, 'Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework Towards a More Robust Protection of Individuals' (2017)
<https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf> accessed 30 September 2018

Mallory S, 'The Concept of Asymmetrical Policing' (2007) 12 Policing Working Paper Series

Moerel L and Prins C, 'Privacy for the Homo Digitalis, Proposal for a new Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (2016)
<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123> accessed 10 April 2018

***(iv) Reports***

Bignami F, 'The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens' (Study for the LIBE Committee, European Parliament 2015)
<http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf> accessed 30 September 2018

Boehm F, 'A comparison between US and EU Data Protection Legislation for Law Enforcement,' (Study for the LIBE Committee, European Parliament 2015)
<http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf> accessed 30 September 2018

Boehm F and Cole M, 'Data Retention after the Judgement of the Court of Justice of the European Union' (2014) Report for the Greens, European Free Alliance, in the European Parliament
<https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf> accessed 1 August 2017

Cannataci J, 'Study on Recommendation No. R(87)15 of 17 September 1987 Regulating the Use of Personal Data in the Police Sector 'Data Protection Vision 2020- Options for Improving European Policy and Legislation during 2010-2020' (2010), 22nd Meeting 15-17 November 2010, Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, T-PD-BUR (2010) 12 final
<https://www.um.edu.mt/library/oar/bitstream/handle/123456789/26239/JACannataciReporttoCouncilofEuropecompletewithAppendices31Oct2010.pdf?sequence=1&isAllowed=y> accessed 30 September 2018

Cannataci J and Caruana M, 'Recommendation R (87)15: Twenty-Five Years Down the Line' (2013), Report to the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data T-PD (2013) 11
<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e7a3c> accessed 30 September 2018

Cavoukian A, 'Privacy by Design, The 7 Foundational Principles' (2009)
<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf> accessed 30 September 2018

Cavoukian A, *'Privacy by Design* in Law, Policy and Practice' A White Paper for Regulators, Decision-Makers and Policy-Makers (2011)
<http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf> accessed 30 November 2018

De Hert P, 'Biometrics: Legal Issues and Implications', Background Paper for the Institute of Prospective Technological Studies, DG JRC- Sevilla European Commission (2005)

Enterprise Privacy Group, 'Privacy by Design: An Overview of Privacy Enhancing Technologies' (2008)
<http://www.dsp.utoronto.ca/projects/surveillance/docs/pbd_pets_paper.pdf> accessed 30 December 2018

Greer, 'Exceptions to Articles 8 to 11 of the European Convention on Human Rights' (1997)
<http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf> accessed 10 April 2018

Schlehahn E, Marquenie T, and Kindt E, 'Data Protection Impact Assessments (DPIAs) in the Law Enforcement Sector according to Directive (EU) 2016/680- A Comparative Analysis of Methodologies' (2016) Deliverable for the VALCRI project (Visual Analytics for Sense-Making in Criminal Intelligence Analysis)
<http://valcri.org/our-content/uploads/2018/06/VALCRI-DPIA-Guidelines-Methodological-Comparison.pdf > accessed 30 December 2018

***(v) Newspaper Articles***

Andriole S, 'Facebook's Zuckerberg Quietly Drops Another Privacy Bomb- Facial Recognition' *Forbes* (12 April 2018)
<https://www.forbes.com/sites/steveandriole/2018/04/12/facebooks-zukerberg-quietly-drops-another-privacy-bomb-facial-recognition/#27ebe7fe51c0> accessed 30 September 2018

Bradshaw T, 'Facebook Ends Facial Recognition in Europe' *Financial Times* (21 September 2012)
<https://www.ft.com/content/fa9c4af8-03fc-11e2-b91b-00144feabdc0> accessed 30 September 2018

Cagle, M, 'Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color' *ACLU Northern California* (11 October 2016)
<https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target> accessed 30 September 2018

Chan C, 'What Facebook Deals with Everyday: 2.7 Billion Likes, 300 Million Photos Uploaded and 500 Terabytes of Data' *Gizmodo* (22 August 2012)
<https://gizmodo.com/5937143/what-facebook-deals-with-everyday-27-billion-likes-300-million-photos-uploaded-and-500-terabytes-of-data> accessed 30 September 2018

Grossman W, 'Is School Fingerprinting out of Bounds?' *The Guardian* (30 March 2006) <https://www.theguardian.com/technology/2006/mar/30/schools.guardianweeklytechnologysection> accessed 30 September 2018

Lunden I, 'Facebook Turns Off Facial Recognition in the EU, Gets the All-Clear on Several Points from Ireland's Data Protection Commissioner on its Review' *TechCrunch* (21 September 2012) <https://techcrunch.com/2012/09/21/facebook-turns-off-facial-recognition-in-the-eu-gets-the-all-clear-from-irelands-data-protection-commissioner-on-its-review/> accessed 30 September 2018

Mizroch A, 'PayPal Wants You to Inject Your Username and Eat Your Password' *the Wall Street Journal* (17 April 2015) <http://blogs.wsj.com/digits/2015/04/17/paypal-wants-you-to-inject-your-username-and-eat-your-password/> accessed 30 May 2016

Petroff A, 'MasterCard Launching Selfie Payments' *CNN* (22 February 2016) <http://money.cnn.com/2016/02/22/technology/mastercard-selfie-pay-fingerprint-payments/> accessed 30 May 2016

Pidd H, 'Facebook Facial Recognition Software Violates Privacy Laws, Says Germany' *The Guardian* (3 August 2011) <https://www.theguardian.com/technology/2011/aug/03/facebook-facial-recognition-privacy-germany> accessed 30 September 2018

Press Association, 'Facebook Faces Fines up to £80K' *The Guardian* (21 September 2012) <https://www.theguardian.com/technology/2012/sep/21/facebook-faces-privacy-fine> accessed 30 September 2018

__ __ 'Facebook Receives Nearly 2,000 Data Requests from UK Police' *The Guardian* (11 April 2014) <https://www.theguardian.com/technology/2014/apr/11/facebook-2000-data-requests-police> accessed 30 September 2018

Quiñonero Candela J, 'Managing Your Identity on Facebook with Face Recognition Technology' *Facebook Newsroom* (19 December 2017) <https://newsroom.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/> accessed 10 April 2018

Ram A, 'Tech Companies Endure Near-Doubling of Requests for Personal Data' *Financial Times* (30 August 2017) <https://www.ft.com/content/b754882e-8cbd-11e7-9084-d0c17942ba93> accessed 10 April 2018

Sengupta S, 'Facebook's Prospects May Rest on Trove of Data' *New York Times* (14 May 2012) <https://www.nytimes.com/2012/05/15/technology/facebook-needs-to-turn-data-trove-into-investor-gold.html?pagewanted=all> accessed 30 September 2018

Stewart T, 'Facebook is Using GDPR as a Means to Bring Facial Recognition Back to Europe' *MobileMarketing* (18 April 2018)

<https://mobilemarketingmagazine.com/facebook-facial-recognition-eu-europe-gdpr-canada> accessed 30 September 2018

Wollacott E, 'Protection when Tech Gets Rather Personal', Biometrics and Identity Management' *Le Raconteur* (30 April 2015)
<https://www.raconteur.net/biometrics-2015> accessed 30 May 2016

***(vi) Miscellaneous***

____ 'The Biometrics for Banking: Market and Technology Analysis, Adoption Strategies and Forecasts 2018-2023- Second Edition' (businesswire.com, 29 June 2018)
<https://www.businesswire.com/news/home/20180629005676/en/Biometrics-Banking-2018-Market-Technology-Analysis-Adoption> accessed 30 September 2018

Adler A, 'Can Sample Images be Regenerated from Biometric Templates?' (Biometrics Conference, 22-23 September 2003)
<http://www.sce.carleton.ca/faculty/adler/publications/2003/adler-2003-biometrics-conf-regenerate-templates.pdf> accessed 30 May 2016

Afonin O, 'Government Request Reports: Google, Apple and Microsoft' (*ElcomSoft* blog, 16 January 2017)
<https://blog.elcomsoft.com/2017/01/government-request-reports-google-apple-and-microsoft/> accessed 1 August 2017

Apple's Transparency Report, 'Report on Government and Private Party Requests for Customer Information, January 1- June 30, 2017) [2017]
<https://images.apple.com/legal/privacy/transparency/requests-2017-H1-en.pdf/> accessed 10 April 2018

Ayer E, 'How Government Biometrics are Moving into the Private Sector' (*Biometric Update*, 28 June 2017)
<https://www.biometricupdate.com/201706/how-government-biometrics-are-moving-into the-private-sector> accessed 30 September 2018

Baratta R, 'Complexity of EU law in the domestic implementing process' (Speech at the 19th Quality of Legislation Seminar 'EU Legislative Drafting: Views from those applying EU law in the Member States', 3 July 2014)
<http://ec.europa.eu/dgs/legal_service/seminars/20140703_baratta_speech.pdf> accessed 10 April 2018

BioPrivacy, FAQs 'Are Biometrics Unique Identifiers?'
<http://www.bioprivacy.org > accessed 30 May 2016

Brewczyńska M, 'the Principle of Accountability in the General Data Protection Regulation: Calling the EU Legislator to Account for Limiting the Wording of Article 5(2) GDPR to Data Controllers' [2018] (LL.M thesis)
<arno.uvt.nl/show.cgi?fid=144595> accessed 30 September 2018

Bromba M, 'On the Reconstruction of Biometric Raw Data from Template Data' (2006) <http://www.bromba.com/knowhow/temppriv.htm> accessed 30 May 2016

Facebook's Transparency Report [2017]
<https://newsroom.fb.com/news/2017/12/reinforcing-our-commitment-to-transparency/> accessed 10 April 2018

_____ half-year [2018]
<https://transparency.facebook.com/government-data-requests> accessed 10 April 2018

Google's Transparency Report [2018]
<https://transparencyreport.google.com/user-data/overview > accessed 10 April 2018

Korff, D 'The Standard Approach under Articles 8-11 ECHR and Article 2 ECHR' (2009)
<http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf > accessed 10 April 2018

Larduinat X, 'Biometrics and the Next Financial Sector Revolution' (*blog.Gemalto*, 22 May 2018)
<https://blog.gemalto.com/financial-services/2018/05/22/biometrics-and-the-next-financial-sector-revolution/> accessed 30 September 2018

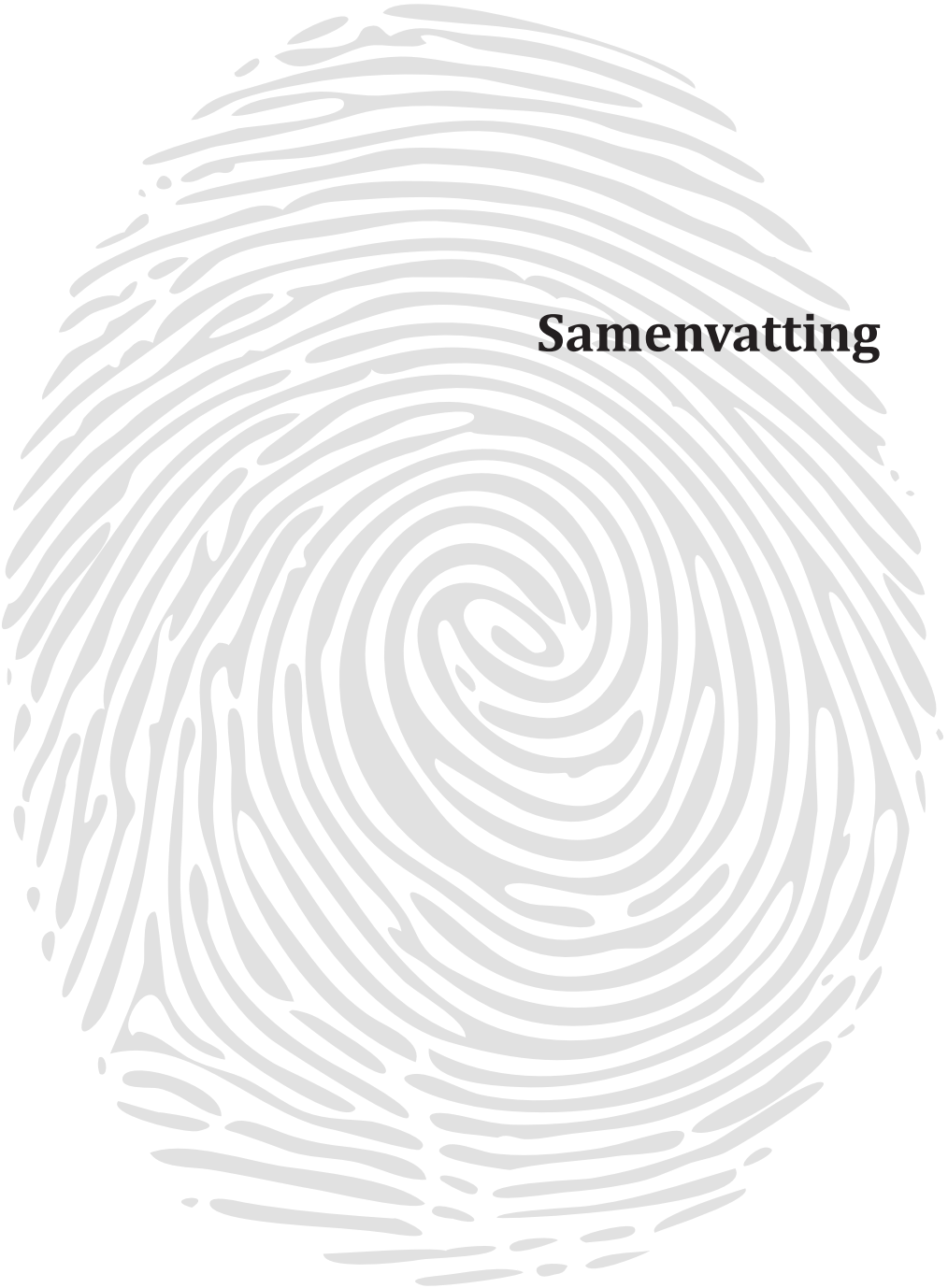
LeBlanc J, 'Kill All Passwords' (2015)
<http://www.slideshare.net/jcleblanc/kill-all-passwords> accessed 30 May 2016

Microsoft's Transparency Report [2018]
<https://www.microsoft.com/en-us/about/corporate-responsibility/lerr/> accessed 10 April 2018

Microsoft, Law Enforcement Requests Report
<https://www.microsoft.com/about/csr/transparencyhub/lerr > accessed 10 April 2018

Stalla-Bourdillon S, 'the GDPR and the Biggest Mess of All: Why Accurate Legal Definitions Really Matter…' blogpost (*Peep Beep*, 12 April 2016)
<https://peepbeep.wordpress.com/2016/04/12/the-gdpr-and-the-biggest-mess-of-all-why-accurate-legal-definitions-really-matter/> accessed 30 May 2016

Woods L, 'Data Retention and National Law: the ECJ Ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)' (*EU Law Analysis*, 21 December 2016)
<http://eulawanalysis.blogspot.nl/2016/12/data-retention-and-national-law-ecj.html> accessed 1 August 2017



# Samenvatting

Biometrische technologieën zijn overal in ons dagelijks leven. Lange tijd werden zij slechts ingezet door de rechtshandhavingsautoriteiten (hierna ten behoeve van de leesbaarheid: politie) en bij grenscontroles, maar biometrische technologieën worden tegenwoordig ook veel gebruikt door private partijen. Vingerafdrukken, gezichtsscans, stem- en irisherkenning worden allen gebruikt om transacties te voltooien, toegang te krijgen tot werkplekken, en om mobiele apparaten mee te ontgrendelen. Sociale media bevatten ook een grote hoeveelheid persoonlijke gegevens, waarvan sommige (zoals gezichtsafbeeldingen) kunnen worden omgewerkt voor biometrische herkenningsdoeleinden. Omdat deze gegevens gebruikt kunnen worden om personen mee te identificeren, vormen zij een zeer waardevolle bron voor de politie.

Dit proefschrift richt zich op het toenemende hergebruik van persoonsgegevens die oorspronkelijk voor een ander doel verzameld zijn. In het bijzonder focust het zich op het politiegebruik van biometrische gegevens die door private partijen verzameld zijn. Zo wordt nagegaan of de nieuwe EU-regels voor gegevensbescherming voldoende waarborgen bieden aan personen in dit scenario. De onderzoeksvraag luidt als volgt:

> *Welke waarborgen biedt het nieuwe EU-kader voor gegevensbescherming aan natuurlijke personen van wie biometrische gegevens, die oorspronkelijk door private partijen verzameld zijn, verwerkt worden voor politiedoeleinden door bevoegde autoriteiten?*

Voordat het huidige EU-kader voor gegevensbescherming werd aangenomen, waren de regels voor de verwerking van persoonsgegevens verdeeld tussen de Richtlijn Gegevensbescherming (Richtlijn 95/46/EG) en een lappendeken van verschillende instrumenten die van toepassing waren op politiële en justitiële samenwerking. Dit gefragmenteerde juridische kader is vervangen door één instrument dat van toepassing is op de verwerking van persoonsgegevens in alle sectoren (Verordening 2016/679, de Algemene Verordening Gegevensbescherming of de AVG) en één meer specifieke richtlijn voor de verwerking van persoonsgegevens in de politiële en strafrechtelijke context (Richtlijn 2016/680, of de 'Politie'-Richtlijn). De kern van het onderzoek wordt gevormd door het raakvlak tussen deze twee instrumenten en de gevolgen daarvan voor de waarborgen voor natuurlijke personen.

Dit boekwerk bestaat uit vier gepubliceerde artikelen en één nog niet gepubliceerd artikel, waarin een aantal belangrijke bevindingen zijn gedaan. Ten eerste heeft het onderzoek aangetoond dat er een grote afstand bestaat tussen de juridische en technische definities van het kernbegrip 'biometrische gegevens.' Wat bij het begin van het onderzoek een terminologisch probleem leek te zijn, werd een kritische discussie over de reikwijdte van het begrip naarmate het onderzoek vorderde. Zoals uitgelegd in *hoofdstuk 2*, waren biometrische gegevens niet juridisch gedefinieerd in het oude EU-gegevensbeschermingslandschap. Dit is wel het geval in het nieuwe kader maar, zo is te lezen in *hoofdstuk*

*3*, de wettelijke definitie van biometrische gegevens is onnauwkeurig en staat los van de wetenschappelijke betekenis. De analyse toont verder, op basis van de definitie van biometrische gegevens (artikel 4, lid 14, AVG) en van een overweging waarin wordt bepaald wanneer foto's biometrische gegevens bevatten (overweging 11 AVG), inconsistenties aan in de betekenis van 'unieke identificatie.' Dit proefschrift stelt dat 'unieke identificatie' met betrekking tot biometrische gegevens moet worden begrepen vanuit het oogpunt van gegevensbescherming in plaats van de biometrische identificatiemodaliteit. Het bepalen van de betekenis van deze 'unieke identificatie' is cruciaal omdat het criterium ook wordt gebruikt om biometrische gegevens te kunnen classificeren als gevoelige gegevens. Volgens artikel 9, lid 1 AVG en artikel 10 van de 'Politie'-Richtlijn zijn alleen biometrische gegevens die worden verwerkt om een natuurlijke persoon 'uniek te identificeren' gevoelige gegevens.

Na deze behandeling van de wettelijke en technische achtergrond, bespreekt de studie het scenario waarin de politie persoonlijke gegevens verwerkt die zijn verzameld door particuliere partijen. De *hoofdstukken 4* en *5* richten zich op het raakvlak tussen de AVG en de 'Politie'-Richtlijn. Hoewel de AVG van toepassing is op de verzameling van persoonsgegevens door private partijen, zijn de regels in de 'Politie'-Richtlijn van toepassing op het latere gebruik van deze gegevens door de politie voor een wetshandhavingsdoeleind. Geen van beide instrumenten biedt echter duidelijke regels over de status van het latere gebruik van AVG-gegevens door de politie.

*Hoofdstuk 4* onderzoekt of de 'Politie'-Richtlijn adequate waarborgen biedt aan personen van wie de persoonsgegevens, verzameld onder de AVG, opnieuw worden verwerkt volgens de 'Politie'-Richtlijn. De analyse bouwt voort op de jurisprudentie van het Europees Hof van Justitie (hierna: het Hof) inzake de zogenaamde gegevensretentieverplichting en meer specifiek op *Digital Rights Ireland* en *Tele2Sverige*. De scenario's die aan de oorsprong liggen van deze beslissingen van het Hof zijn anders dan welke in dit proefschrift behandeld worden. In het geval van gegevensretentie zijn private partijen wettelijk verplicht om de verzamelde gegevens te bewaren, zodat de politie hier toegang toe kan krijgen en deze kan verwerken. Aangezien het Hof duidelijk onderscheid maakte tussen retentie en toegang/hergebruik, wordt in dit onderzoek naar analogie van de bevindingen van het Hof met betrekking tot dit tweede aspect geredeneerd. Als gevolg hiervan komt deze studie tot de conclusie dat de 'Politie'-Richtlijn mogelijk geen afdoende procedurele en wezenlijke waarborgen biedt. In het bijzonder schiet de Richtlijn tekort op de volgende punten: de definitie van 'objectieve criteria' die de voorwaarden voor toegang en gebruik door wetshandhavers bepaalt; de specifieke procedurele voorschriften betreffende het vooronderzoek van een toegangsverzoek, en de formulering van het recht op informatie. Met betrekking tot het laatste punt oordeelde het Hof dat natuurlijke personen wiens gegevens door de politie zijn geraadpleegd hierover moeten worden geïnformeerd. Hiermee mag gewacht worden totdat lopend onderzoeken niet langer geschaad zouden kunnen

worden. Deze kennisgeving geeft de betrokkenen de mogelijkheid om een beroep in te stellen bij een rechter, evenals de mogelijkheid om gebruik te maken van andere rechten (zoals het recht van toegang). In het onderzoek rijzen twijfels over de vraag of het recht op informatie, zoals geformuleerd in artikel 13 van de 'Politie'-Richtlijn, rechtshandhavingsinstanties verplicht om personen ervan in kennis te stellen dat hun gegevens zijn verwerkt. Sommige auteurs menen dat artikel 13, lid 2, deze verplichting zou kunnen overnemen. Deze bepaling verwijst echter noch naar een meldingsplicht, noch naar een specifiek tijdstip waarop een dergelijke kennisgeving moet worden gedaan. Ten slotte bespreekt *hoofdstuk 4* kort de rol van het doelbindingsprincipe als een waarborg bij het hergebruiken van persoonsgegevens over de twee instrumenten. Dit laatste punt vormt de overgang naar het volgende hoofdstuk, dat volledig op dat principe gericht is.

De analyse van de bepalingen in de AVG en de 'Politie'-Richtlijn toont aan dat het doelbindingsprincipe geen duidelijke rol speelt in het geval van (her)verwerking die de beide instrumenten kruist. Deze conclusie is om minstens twee redenen problematisch. Ten eerste maakt het beginsel deel uit van het fundamentele recht op gegevensbescherming dat is vastgelegd in artikel 8 van het Handvest van de Grondrechten van de Europese Unie. Op deze manier zou het een garantie moeten vormen voor de bescherming van persoonlijke gegevens. Ten tweede heeft het principe tot doel om de voorwaarden voor de verdere verwerking van persoonsgegevens in te kaderen. Afwijkingen en uitzonderingen op het principe zijn mogelijk; de verwerking moet dan echter voldoen aan specifieke voorwaarden. *Hoofdstuk 5* concludeert dat het scenario waar dit proefschrift op focust noch deel uitmaakt noch wordt opgehelderd in een overweging van één van de beide instrumenten. Het lijkt er zelfs op dat een keuze hierover opzettelijk is vermeden, zodat de lidstaten vrij kunnen beslissen hoe zij de herverwerking van AVG-persoonsgegevens op grond van de regels uit de 'Politie'-Richtlijn inrichten. Deze situatie legt de kloof tussen de twee instrumenten bloot en werpt licht op de problemen die worden veroorzaakt door de splitsing van regels tussen twee verschillende instrumenten.

Afsluitend analyseert dit onderzoek gegevensbescherming door ontwerp en standaardinstellingen (*data protection by design and by default*) en gegevensbeschermingseffectbeoordelingen (*data protection impact assessments*, hierna: GBEB) in een poging om aanbevelingen te doen. Beide maatregelen zijn in het nieuwe EU-kader voor gegevensbescherming geïntroduceerd als verantwoordingsinstrumenten voor de verwerkingsverantwoordelijken. Zoals in *hoofdstuk 6* wordt gesuggereerd, kunnen deze hulpmiddelen ook extra waarborgen bieden voor natuurlijke personen wiens gegevens opnieuw worden verwerkt voor politiedoeleinden. Noch de AVG, noch de 'Politie'-Richtlijn biedt echter specifieke richtsnoeren voor de toepassing of uitvoering ervan. Gegevensbescherming door ontwerp en standaardinstellingen zijn overkoepelend principes die zowel gegevensbeschermingsbeleid als specifiek oplossingen voor het behoud van privacy kunnen omvatten (zoals versleuteling en anonimisering). GBEBs zijn een aanvullend hulpmiddel dat

alleen wordt gebruikt als een verwerkingshandeling 'waarschijnlijk tot een hoog risico' leidt voor de rechten en vrijheden van natuurlijke personen. Hoewel de AVG richtlijnen bevat over wat een 'hoog risico' kan vormen, ontbreken deze in de 'Politie'-Richtlijn. Meer in het bijzonder wordt 'elk type verwerking van biometrische gegevens' niet als 'hoog risico' beschouwd. Volgens het Europees Comité voor gegevensbescherming leidt de verwerking van biometrische gegevens alleen tot een GBEB als de verwerking leidt tot gevoelige gegevens (d.w.z. biometrisch gegevens worden verwerkt om een persoon uniek te identificeren) en/of een ander criterium aanwezig is (zoals verwerking op grote schaal of resulterend systematisch toezicht). Op basis van deze beschouwing van de bepalingen van beide instrumenten, wordt in *hoofdstuk 6* opgeroepen om de politieverwerking van biometrische gegevens die zijn verzameld door private partijen te beschouwen als 'hoog risico'-proces dat de verplichting tot het uitvoeren van een GBEB teweegbrengt.

Een gezaghebbende interpretatie van de nieuwe regels is noodzakelijk. Zoals voorgesteld in de verschillende hoofdstukken van het onderzoek, kunnen hiervoor verschillende paden worden bewandeld, ook al lijkt het dat geen van hen de perfecte oplossing biedt. Ten eerste zou het Europees Comité voor Gegevensbescherming (dat de Groep Gegevensbescherming Artikel 29 vervangt) aanbevelingen en richtsnoeren kunnen uitvaardigen om te verduidelijken wat de reikwijdte van de regels is en wat de voorwaarden zijn waaronder biometrische gegevens als gevoelige gegevens worden beschouwd. Er zijn voorts richtsnoeren nodig met betrekking tot de regels die van toepassing zijn op de verwerking van persoonsgegevens die de twee instrumenten kruist. De richtlijnen en aanbevelingen van het Europees Comité zijn echter niet bindend. Ten tweede, aangezien Richtlijn 2016/680 in de lidstaten is geïmplementeerd, kunnen nationale rechtbanken prejudiciële vragen stellen aan het Hof van Justitie op basis van nationale bepalingen. Hoewel dit pad de rechtszekerheid het beste waarborgt, zal dit een lange weg zijn en zal het de ijver van een activistische burger vereisen om een gerechtelijke procedure op nationaal niveau te starten.